

VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS KATEDRA

Magistro baigiamasis darbas

Abonento atpažinimo modulio įrankių rinkinys (SAT SIM)

Subscriber Identity Module Application Toolkit (SAT SIM)

Atliko: IIM kurso, 2 grupės studentas

Džiugas Baltrūnas (parašas)

Darbo vadovas:

Tomas Kaulakys (parašas)

Recenzentas:

Arūnas Janeliūnas (parašas)

Vilnius
2007

Turinys

Turinys	2
Sutrumpinimų sąrašas	4
Įvadas	6
1. Literatūros apžvalga	9
1.1. SIM kortelė ir jos sandara	9
1.1.1. Fizinė architektūra	10
1.1.2. Programinės įrangos architektūra	10
1.1.3. Failinė sistema	11
1.1.4. APDU	12
1.1.5. SIM komandos	13
1.1.6. Saugumas	14
1.1.7. Standartai	15
1.2. SIM įrankinių rinkinys – SAT	16
1.2.1. Proaktyviosios komandos	16
1.2.2. Prenumeruojami įvykiai	19
1.3. Java kortelė – Java Card	20
1.4. SIM valdymas nuotoliniu būdu – OTA	22
1.4.1. Nuotolinis failų valdymas – RFM	24
1.4.2. Nuotolinis taikomųjų programų valdymas – RAM	25
2. Esamų STK programų problemų apžvalga	27
3. StartDial projektas	29
3.1. StartDial reikalingumas	29
3.2. Techniniai reikalavimai	30
3.3. Galimų modelių analizė	31
3.3.1. Serverine dalimi paremtas sprendimas	31
3.3.2. SIM kortele paremtas sprendimas	31
3.4. StartDial programos savybės	32
3.5. StartDial architektūra	32
3.6. StartDial apletas	33
3.7. StartDial serverinė dalis	34
3.7.1. Duomenų bazės schema	35
3.7.2. OTA mechanizmai	36
3.8. Testavimas	37

3.9.	Galimos papildomos funkcijos bei savybės.....	39
4.	Mobilusis elektroninis parašas.....	41
4.1.	WTLS ir WIM.....	41
4.2.	STK saugumo mechanizmai.....	44
4.3.	Java Card saugumo sąsajos	45
4.3.1.	javacard.security klasės	46
4.3.2.	javacard.security interfeisai	46
4.3.3.	Java Card specifikacijos versijos ir realizacija	47
4.4.	SATSA / JSR 177	48
4.5.	Išvados	51
5.	Tolimesni darbai	53
	Išvados.....	54
	Summary	57
	Literatūros ir šaltinių sąrašas	58
	Priedas nr. 1. StartDial testinių duomenų paruošimo skriptas	60

Sutrumpinimų sąrašas

EEPROM	Electrically Erasable Programmable Read-Only Memory (elektriškai ištrinama programuojama pastovios programos atmintis)
GSM	Global System for Mobile communications (mobiliojo ryšio sistema)
SAT	SIM Application ToolKit (SIM įrankių rinkinys)
SIM	Subscriber Identity Module (abonento atpažinimo modulis)
ROM	Read Only Memory (atmintis tik skaitymui)
RAM	Remote Application Management (nuotolinis prg. valdymas)
RFM	Remote File Management (nuotolinis failų valdymas)
STK	SIM ToolKit (SIM įrankių rinkinys)
ME	Mobile Equipment (mobilusis įrenginys)
DF	Dedicated File (dedikuotasis failas)
EF	Elementary File (elementarusis failas)
AID	Application Identifier (taikomosios prg. identifikatorius)
JCRE	Java Card Runtime Environment (Java Card paleidimo aplinka)
APDU	Application Protocol Data Unit (protokolo duomenų vienetas)
SW	Status Word (būsenos žodis)
CHV	Card Holder Verification (kortelės savininko verifikavimas)
PIN	Personal Identifier (asmeninis identifikatorius)
PUK	Personal Unblock Key (PIN atblokovimo kodas)
OTA	Over The Air (nuotolinė belaidė komunikacija)
URL	Uniform Resource Locator (adresas internete)
SATSA	Security and Trust Services API for J2ME (J2ME saugumo sąsaja)
BIP	Bearer Independent Protocol (nuo duomenų pernešėjo nepriklausantis protokolas)
SSL	Secure Sockets Layer (saugus interneto protokolas)
TLS	Transport Layer Security (saugus interneto protokolas)
PKI	Public Key Infrastructure (viešojo rakto infrastruktūra)
wPKI	Wireless Public Key Infrastructure (bevielė viešojo rakto infrastruktūra)
HTTPS	Hyper Text Transfer Protocol Secure (saugus HTTP protokolas per SSL)
J2ME	Java 2 Platform, Micro Edition (Java mobilioji redakcija)
J2SE	Java 2 Platform, Standard Edition (Java standartinė redakcija)

WTLS	Wireless Transport Layer Security (bevielio transporto sluoksnio apsaugos protokolas)
WIM	Wireless Application Protocol Identity Module (WAP identifikacijos modulis WIM)

Ivadas

Magistro darbo metu bus koncentruojamasi į antrosios mobiliojo ryšio kartos (2G, 2.5G) intelektualiąją kortelę – abonto atpažinimo modulį SIM, taikomųjų programų rinkinį STK bei antrosios kartos SIM kortelėse atsiradusią proaktyvių (angl. proactive) komandų sąvoką. Pastarųjų komandų, apibrėžtų [GSM 11.14] standarte, pagalba STK programos, veikiančios SIM kortelėje, gali siųsti komandas telefono įrenginiui. Komandos yra vadinamos proaktyviomis todėl, kad jų loginis iniciatorius yra SIM kortelė, nors realiai tokios komandos yra atsakymas į prieš tai iš ME gautą ir įvykdytą komandą. Parodyti tekstą ME ekrane, užmegzti dialogą su ME vartotoju, išsiųsti trumpąją SMS žinutę – tai tik keletas proaktyvių komandų pavyzdžių.

Probleminė sritis

STK programos, generuodamos proaktyvias komandas ir apdorodamos jų rezultatus, atveria plačias galimybes pridėtinės vertės mobiliųjų paslaugų sukuriui. Lyginant su kitomis pridėtinės vertės paslaugomis, pavyzdžiui, MMS žinutėmis ar vaizdo transliacijomis realiu laiku, galima teigti, jog STK programos turi kur kas platesnį suderinamumą su rinkoje esančiais mobiliaisiais telefonais. Nors SIM operacinė sistema yra ribojama palyginti nedidelės spartos procesoriaus bei atminties resursų, STK programų pagalba gali būti sprendžiami šių probleminių sričių keliami uždaviniai: mobilioji komercija ir mobilūs mokėjimai, mobilus elektroninis parašas, saugus mobiliojo turinio paskirstymas, asmeninė duomenų saugykla, informacija pagal užklausimą ir nemažai kitų.

Nepaisant to, kad šiuo metu didžioji dalis rinkoje esančių SIM kortelių yra antrosios kartos ir palaiko proaktyvias komandas, STK programų kūrimas ir diegimas iki šiol tebėra aktuali problema. Tai visų pirma lemia mobiliojo ryšio rinkos dalyvių specifika. Paprastai mobiliojo ryšio operatorius SIM korteles perka iš vieno ar kelių SIM kortelių gamintojų (pvz. Gemalto, Oberthur, Orga ir kt.) su iš anksto sutartu STK programų rinkiniu, atsisakant tokių programų kūrimo delegavimo trečiosioms šalims. Tokį atsisakymą nulemia du pagrindiniai veiksniai – operatoriaus keliami saugumo reikalavimai bei paieška tokių trečiųjų šalių, kurios realiai galėtų tuos reikalavimus patenkinti bei užtikrinti sukurto produkto maksimalų suderinamumą su mobiliaisiais įrenginiais. Trečiosioms šalims savo ruožtu suderinamumo užtikrinimas yra sunkiai įmanomas dėl SIM kortelių gamintojų naudojamų technologijų, kurios daugeliu atveju yra uždaros arba griežtai nesilaiko standartų, todėl sukurtas STK paremtas produktas dažniausiai yra nesuderinamas tarp skirtingų gamintojų SIM kortelių.

Kaip vieną iš galimybių, leidžiančių spręsti minėtas problemas, būtina nagrinėti Java Card technologiją – standartą, leidžiantį lustus programuoti Java programavimo kalba. Pagrindiniai šios technologijos privalumai yra nepriklausomumas nuo platformos¹, kelių taikomųjų programų vienoje kortelėje palaikymas, galimybė įdiegti naujas bei atnaujinti esamas programas, lankstus bei populiarus programavimas objektiškai orientuota Java kalba bei suderinamumas su egzistuojančiais „gudriųjų kortelių“ standartais. Kelių didžiųjų mobiliojo ryšio operatorių iniciatyva buvo patvirtintas Java Card technologijos naudojimo SIM kortelėse standartas [GSM 03.19]. Jame yra numatytos taikomųjų programų proaktyvių komandų bei failinės sistemos valdymui skirtos sąsajos, kurias galima naudoti Java Card STK programoms.

Nors Java yra gerai žinoma savo paradigma „rašyk kartą, vykdyk bet kur“, o į rinką išleistų Java Card SIM kortelių skaičius jau skaičiuojamas milijonais, STK programų kūrimo ir diegimo sudėtingumas sumažėjo palyginti nežymiai. Neatsirado ir atviros bendruomenės, vienijančios STK programų kūrėjus. Vis dar tebėra kompliktuotas programų diegimas, duomenų apsikeitimas per OTA saugumo sritis (angl. security domains).

Šiandien ne mažiau aktualūs ir elektroninio parašo klausimai. Mobiliojo ryšio infrastruktūra įgalina elektroniniam parašui būtiną autentifikacijos ir pasirašymo įranga perkelti į mobilių telefoną, o SIM kortelę naudoti kaip saugią raktų laikmeną. Nepaisant to, kad Elektroninio parašo įstatymas Lietuvoje priimtas dar 2000 m., mažai pasistūmėta įgyvendinant konkrečius wPKI (bevielės viešojo rakto infrastruktūros) modelius. Įgyvendinant mobilaus elektroninio parašo priemones SIM kortelėje (privataus rakto, atitinkančio kvalifikuotą sertifikatą, saugojimas, duomenų perdavimo ir pasirašymo modeliai ir kt.), būtini susitarimai dėl standartų bei technologijų tiek tarp mobiliojo ryšio operatorių, tiek tarp kitų wPKI dalyvių.

Darbo tikslai ir uždaviniai

Manome, kad sprendžiant minėtus probleminės srities klausimus yra reikalinga atlikti išsamią su šia sritimi susijusių technologijų analizę, įvertinti kiekvienos iš technologijų privalumus bei trūkumus, taip pat įvardinti pagrindines problemas ir galimus jų sprendimo būdus.

Kadangi SIM kortelė yra neatsiejamas kiekvieno mobiliojo ryšio paslaugų naudotojo elementas, būtina išsiaiškinti, kokie yra SIM kortelėje veikiančių programų reikalavimai bei tipinė architektūra. Savo darbe apsiribosime šiandien tarp intelektualiųjų kortelių (angl.

¹ Java Card taikomosios programos veikia kiekvienoje kortelėje, realizuojančioje Java Card virtualią mašiną.

Smart Card), tame tarpe ir SIM modulio, populiariausia Java Card platforma, kuri yra standartizuota, o programos leidžia kurti Java programavimo kalba. Šios technologijos panaudojimas Lietuvos wPKI infrastruktūroje atvertų platesnes suderinamumo galimybes.

Toliau siekiama išsiaiškinti, kokių konkrečių žingsnių reikia norint sukurti realiai SIM kortelėje veikiančią Java Card taikomąją programą – apletą, bei koks būtų tokios taikomosios programos duomenų modelis ir kaip sprendžiami tų duomenų apsikeitimo su išoriniu pasauliu klausimai. Šiame darbe visų pirma norima parodyti, kad naudojant reikiamas priemones galima sukurti programas, kurios galėtų išspręstų dalį problemų, susijusių su šiandieninėmis mobiliosiomis paslaugomis.

Šių magistro tezių literatūros apžvalgoje (1 skyrius) apžvelgiami literatūros šaltiniai, susiję su SIM kortele, jos sandara, standartais, STK, svarbiausiais Java Card technologijos aspektais bei SIM kortelės valdymu nuotoliniu būdu naudojant OTA mechanizmus. Svarbi skyriaus dalis skiriama tarptautinių standartų, lemiančių STK programų apribojimus, bei aktualiausių probleminių sričių sprendimų studijai.

Pagrindinė darbo dalis (3 skyrius) bus skirta išsamiai proceso, apimančio STK programos kūrimą bei duomenų apsikeitimą OTA mechanizmų pagalba, analizei. Kaip taikomosios Java Card platformoje veikiančios programos pavyzdys, šiame darbe bus detalai nagrinėjamas tarptautiniame SIMAGINE 2006 konkurse antrą vietą užėmęs Java Card projektas „StartDial“, kuris mobilaus telefono vartotojo skambučius tam tikrais numeriais pakeičia telefono WAP naršyklės paleidimu su konkrečiu įvestą numerį (toliau – trumpinį) atitinkančiu WAP adresu (URL). Visų pirma aptarsime StartDial projekto reikalingumą, tuomet pateiksime galimus architektūros modelius, kiekvieno iš jų privalumus bei trūkumus ir detalai išanalizuosime pasirinktąjį – SIM kortele paremtąjį modelį. Bus aprašomos dvi sprendimo dalys – serverinė (centrinė duomenų bazė, OTA mechanizmai) ir SIM kortelės (Java Card apletas, jo veikimo principai).

Paskutinė šio darbo dalis (4 skyrius) yra skirta su mobiliuoju elektroniniu parašu susijusių technologijų apžvalgai. Bus nagrinėjami pagrindiniai STK saugumo aspektai, Java Card saugumo sąsajos bei galimybė J2ME taikomosioms programoms bendrauti su SIM kortele.

Tikimasi, kad sėkmingai atlikus darbą bus išskirtos ir išanalizuotos svarbiausios problemos, lemiančios STK programų kūrimo problematiką ir mobiliojo elektroninio parašo ypatumus bei pateikti pasiūlymai kai kurių specifinių problemų sprendimui.

Paskutiniame šio darbo skyriuje „Tolimesni darbai“ trumpai panagrinėsime, kaip išanalizuotas pavyzdinis „StartDial“ projektas bei mobilaus elektroninio parašo technologijų analizė gali pasitarnauti tolimesnėms šios srities studijoms.

1. Literatūros apžvalga

Šiame skyriuje yra pristatoma magistro tezių literatūros apžvalga. Šio skyriaus tikslas yra pamėginti įsigilinti į įvairius literatūros šaltinius ir juose pateikiamus sprendimus, kurie padėtų pasiekti magistro darbe keliamus tikslus – pateikti pasiūlymus, kurie, naudojant tik standartizuotas priemones, leistų sukurti ir įdiegti pridėtinės vertės paslaugą – taikomąją programą – į SIM kortelę, stengiantis neprisirišti prie jos gamintojo, bei leistų tai programai saugiai bendrauti su išorinėmis sistemomis.

Minėtiems tikslams pasiekti šiame skyriuje yra nagrinėjama medžiaga, įskaitant ir tarptautinius standartus, kuri aprašo nagrinėjamą objektą – abonento atpažinimo modulio įrankių rinkinį. Pirmojoje skyriaus dalyje bus detalizuojama pati SIM kortelė, jos sandara ir ją aprašantys standartai. Antrojoje dalyje nagrinėsime STK – SIM įrankių rinkinį, standartuose numatytas proaktyvias komandas. Trečiojoje dalyje aprašysime svarbiausius Java Card aspektus, tame tarpe ir kūrimo procesą, o paskutinėje šio skyriaus dalyje apžvelgsime SIM kortelės valdymą nuotoliniu būdu, naudojant OTA mechanizmus.

Tikimasi, kad sėkmingai atlikta literatūros apžvalga visų pirma leis detaliau susipažinti ir geriau įsisavinti su SAT susijusią medžiagą, reikalingą magistro darbe užsibrėžtiems tikslams pasiekti. Šiame skyriuje, siekiant neprisirišti prie kurios nors vienos uždaros sistemos, daugiausiai dėmesio bus skiriama ne atskirų SIM kortelių gamintojų siūlomų sprendimų, o pačių tarptautinių standartų analizei. Kadangi tokių, su abonento atpažinimo modulio įrankių rinkiniu susijusių standartų yra visa aibė, bus nagrinėjami tik svarbiausi iš jų.

1.1. SIM kortelė ir jos sandara

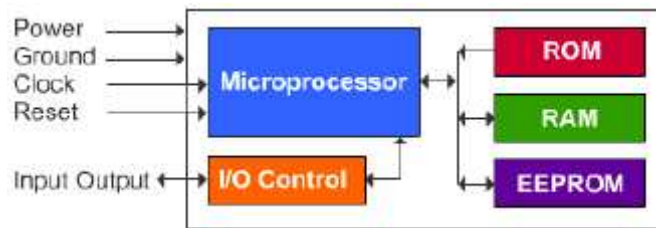
Abonento atpažinimo modulis – SIM – būtinas korinio GSM tinklo komponentas. SIM – tai intelektualioji kortelė (angl. Smart Card), arba kitaip, lustas, kuriame yra saugomi duomenys apie GSM tinklo vartotoją. Pagrindinė SIM kortelės paskirtis yra vartotojo identifikavimas bei saugaus ryšio GSM tinkle užtikrinimas.

Išskiriamos trys SIM kortelių kartos [GC02]. Pirmosios kartos SIM kortelės funkcija yra autentifikacija tinkle bei telefonijos duomenų, tokių kaip telefonų knygelė ar SMS žinutės, saugojimas. Antrosios kartos SIM kortelės pasižymi galimybe kurti pridėtinės vertės paslaugas kaip SIM taikomąsias (angl. SIM Toolkit) STK programas. SIM taikomųjų programų rinkinys bei SIM vartotojo sąsaja yra atitinkamai apibrėžiami [GSM 11.14] ir [GSM 02.19] standartuose. Trečiojoje kartoje SIM tampa viena iš daugelio telefonijos taikomųjų programų UICC lusto platformoje dalimi. Pastarojoje kartoje SIM programos,

vadinamos USIM, pagrindinė paskirtis yra atlikti abipusę (angl. mutual) vartotojo ir tinklo autentifikaciją.

1.1.1. Fizinė architektūra

SIM kortelė priklauso integruotos schemos mikroprocesorinių kortelių (UICC) šeimai. Šios kortelės, lyginant su magnetinėmis ar kitokio tipo kortelėmis, pasižymi didesne duomenų talpykla bei saugumu, kadangi prieiga prie atminties yra kontroliuojama mikroprocesoriaus. SIM kortelė, kaip ir kitos „intelektualiosios“ kortelės, turi ISO 7816 serijos standartais apibrėžtą failinę sistemą, o duomenų apsikeitimas vykdomas taikomųjų programų protokolo duomenų vienetais APDU, kurie aprašyti [ISO 7816-4] standarte.



1 paveikslas. SIM kortelės fizinė architektūra

1 pav. pavaizduota fizinė SIM kortelės architektūra. Svarbiausios jos dalys yra šios:

- CPU – centrinis procesorius;
- ROM – pastovios programos atmintis (ne kaiti);
- EEPROM – elektriškai ištrinama programuojama pastovios programos atmintis (ne kaiti);
- RAM – tiesioginės kreipties atmintis (kaiti).

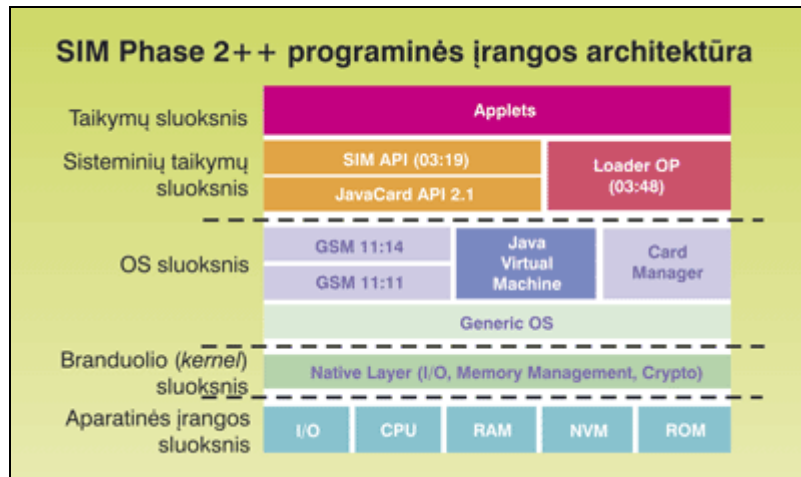
Interfeisą tarp abonento atpažinimo modulio (SIM) ir mobiliojo įrenginio (ME) apibrėžia [GSM 11.11] standartas.

1.1.2. Programinės įrangos architektūra

2 pav. yra pavaizduota SIM programinės įrangos architektūra. Pagrindinės SIM kortelėje veikiančios operacinės sistemos funkcijos yra šios:

- Apsikeitimo tarp kortelės ir išorinio „pasaulio“ valdymas;

- Failų ir duomenų atmintyje valdymas;
- Patikimumo užtikrinimas;
- Kortelės gyvavimo ciklo fazių valdymas;
- Raktų valdymas.



2 paveikslas. SIM programinės įrangos architektūra [RTN01]

1.1.3. Failinė sistema

SIM kortelėms yra būdinga ISO 7816 serijos standartais apibrėžta failinė sistema. Jos pagrindiniai elementai yra šie:

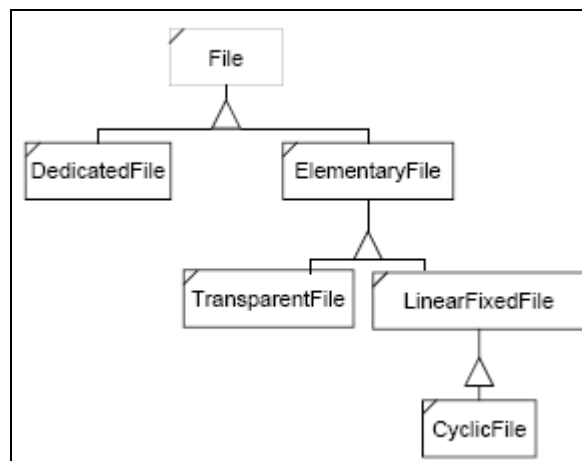
- **DF** - dedikuoti failai (Dedicated Files). Tai katalogo analogas;
- **EF** – elementarieji failai (Elementary Files).

Failinei sistemai yra būdinga klasikinė medžio pavidalo struktūra (žr. 3 pav.), tačiau lyginant su PC paplitusiose failinėse sistemose (pvz. FAT), galioja tokie apribojimai:

- kataloge kartu yra saugomi visų vaikinių failų duomenys;
- katalogo dydis turi būti didesnis už visų failų tame kataloge dydį;
- kiekvienas failas yra identifikuojamas dvibaite reikšme – failo identifikatoriumi FID.

Elementarieji failai yra skirstomi į tris tipus:

- dvejetainiai (angl. binary) failai – tai nuoseklieji failai, kuriuose duomenys neturi papildomos struktūros. Skaitymo ir įrašymo operacijos atliekamos naudojant poslinkį nuo failo pradžios;
- įrašų (angl. record) failai– tai failai, kuriuose yra fiksuoto dydžio įrašai. Tokio failo antraštėje yra saugomas įrašo dydis ir jų kiekis;
- cikliniai (angl. cyclic) failai – įrašų failų poaibio failas, kurio įrašai yra organizuojami kaip ciklinis buferis, t.y. paskutinis įrašas faile rodo į pirmąjį.



3 paveikslas. SIM failinės sistemos struktūra

Vienu laiko momentu prieinamas gali būti tik vienas failas. Jis yra vadinamas einamuoju laiko momentu parinktuoju (angl. selected) failu. Norint dirbti su failu, visų pirma reikia turėti atitinkamas prieigos teises, o prieš pradėdant darbą padaryti failą parinktuoju.

1.1.4. APDU

APDU – tai taikomosios programos duomenų apsikeitimo vienetas. APDU yra žinutė, kuria apsikeičiami duomenys tarp kortelių įrenginio – terminalo ir intelektualiosios kortelės. APDU yra skirstomas į du tipus – įėjties (angl. input) ir išėjties (angl. output). APDU žinutę sudaro 5 baitų ilgio antraštė ir nuo 0 iki 255 baitų duomenų. Struktūriškai APDU formuojamas tokia tvarka:

- **CLA** - klasės baitas. Dažniausia jis unikalus atskirai taikomajai programai;
- **INS** - instrukcijos baitas. Jis nurodo instrukcijos kodą;
- **P1** – pirmasis instrukcijos parametras (priklauso nuo konkrečios instrukcijos);
- **P2** – antrasis instrukcijos parametras (priklauso nuo konkrečios instrukcijos);

- **Lc** – nurodo duomenų ilgį;
- **Duomenys** – 0 – 255 baitų ilgio duomenys, persiusti iš įrenginio į kortelę ar atvirkščiai;
- **Le** – nurodomas ilgis duomenų, kuriuos tikimasi gauti kaip atsakymą iš kortelės.

Kai įrenginys kortelei siunčia APDU komandą, kortelė atsako siųsdama duomenų seką, prasidedančią šiais dviem baitais: SW1 ir SW2. Ši dvibaitė seka vadinama būsenos žodžiu. Jei seka SW1 SW2 yra lygi 0x9000, turime sėkmingai įvykdytą komandą. Visą galimų reikšmių sąrašą galima rasti [ISO 7816-4] standarte.

1.1.5. SIM komandos

[GSM 11.14] standartas aprašo 22 komandas SIM kortelei, kurios yra identifikuojamos APDU klasės baitu A2. Komandos papildomai yra klasifikuojamos į komandas, susijusias su saugumu, komandas operacijoms su failais bei komandas, priklausančias SIM įrankių rinkiniui. 1 lentelėje yra pateiktos šios komandos bei jų paskirtis [RE04].

Komanda	Paskirtis
<i>Saugumo komandos</i>	
CHANGE CHV	Pakeisti PIN.
DISABLE CHV	Atjungti PIN užklausimus.
ENABLE CHV	Įjungti PIN užklausimus.
RUN GSM ALGORITHM	Įvykdyti specifinį GSM kriptografinį algoritmą (naudojama autorizacijai tinkle).
UNBLOCK CHV	Atstatyti PIN pakartotinių bandymų skaitliuką į pradinę reikšmę.
VERIFY CHV	Tikrinti PIN.
<i>Komandos operacijoms su failais</i>	
INCREASE	Padidinti skaitliuko reikšmę faile.
INVALIDATE	Užblokuoti failą (su galimybe atblokuoti).
READ BINARY	Skaityti iš dvejetainio failo.
READ RECORD	Skaityti iš failo su įrašais orientuota struktūra.
REHABILITATE	Atblokuoti failą.
SEEK	Ieškoti tekstinės eilutės įrašais orientuotame faile.
SELECT	Padaryti failą aktyviu.

STATUS	Gauti įvairią informaciją apie šiuo metu aktyvų (angl. selected) failą.
UPDATE BINARY	Rašyti į dvejetainį failą.
UPDATE RECORD	Rašyti į failą su įrašais orientuota struktūra.
<i>SIM įrankių rinkinio komandos</i>	
ENVELOPE	Persiusti duomenis SAT taikomajai programai.
FETCH	Gauti SIM įrankių rinkinio komanda iš SIM kortelės į mobilų įrenginį.
TERMINAL PROFILE	Išvardinti visas mobiliojo įrenginio funkcijas, kurios yra svarbios SIM įrankių rinkiniui.
TERMINAL RESPONSE	Pateikti mobiliojo įrenginio atsaką į prieš tai gautą SIM įrankinių rinkinio komandą.
<i>Kitos komandos</i>	
GET RESPONSE	Komanda, specifinė T=0 protokolui, skirta gauti atsaką iš kortelės.
SLEEP	Nebevartojama komanda, siunčianti intelektualiąją kortelę į energijos taupymo būseną.

1 lentelė. SIM komandos [GSM 11.11]

1.1.6. Saugumas

Vartotojui, norinčiam pasinaudoti SIM kortelės operacijomis ir duomenimis, gali būti taikomi skirtingi saugumo lygiai. Paprastai mobiliojo ryšio kortelė yra apsaugota taip vadinamu kortelės savininko verifikatoriumi – CHV. Šis kodas dar žinomas kaip PIN. Įprasta skirti 4 skirtingus prieigos kodus kortelės savininkui:

- PIN kodas arba CHV1 (nuo 4 iki 8 skaitmenų). PIN kodas apsaugo SIM kortelę nuo neteisėto panaudojimo ir dažniausiai yra suteikiamas kartu su SIM kortele.
- PIN2 kodas arba CHV2 (nuo 4 iki 8 skaitmenų). Kodas gali būti suteiktas kartu su SIM kortele ir skirtas pasiekti tam tikras specialias SIM kortelės funkcijas (pvz. riboto naudojimo adresų knygėlė).
- PUK ir PUK2 (8 skaitmenys). PUK kodas yra reikalingas pakeisti užblokuotą PIN, o PUK2 – PIN2 kodą.

PIN kodo verifikavimui naudojama [GSM 11.14] apibrėžta *VERIFY CHV* APDU komanda. Sėkmingai įvykdžius šią komandą, t.y. APDU duomenyse pateikus teisingą CHV1

ar CHV2 kodą, vartotojui suteikiamas kortelės savininko verifikuotas (angl. default) vartotojo tipas. Iš viso skiriami 8 skirtingi vartotojų tipai:

- Numatytasis – režimas pagal nutylėjimą;
- CHV1 ir CHV2 – kortelės savininko verifikuotas;
- AUT0 – AUT4 – autorizacijos raktas, dar vadinamas ADM raktu.

Kiekvieno elementariojo failo EF antraštėje kiekvienam iš minėtų 8 skirtingų vartotojų tipų yra nurodomos galimos prieigos teisės. Jos yra koduojamos vienu baitu tokiu būdu:

- 0 bitas: skaityti (READ);
- 1 bitas: atnaujinti (UPDATE);
- 2 bitas: vykdyti (EXECUTE);
- 3 bitas: invaliduoti (INVALIDATE);
- 4 bitas: rehabilituoti (REHABILITATE);
- 5-7 bitai: rezervuoti (RFU).

1.1.7. Standartai

2 lentelėje yra pateikti su SIM, STK, Java Card ir OTA susiję standartai. Svarbiausi iš jų yra šie:

- GSM 11.11 – komandos tarp telefono ir SIM kortelės;
- GSM 11.14 – STK specifikacija ir komandų sąrašas;
- GSM 03.19 – Java Card realizacija SIM kortelėje;
- GSM 03.48 – Saugumo mechanizmai: RAM ir RFM per OTA.

Standarto numeris	Pavadinimas
GSM 02.09	Security Aspects
GSM 02.17	SIM, Functional Characteristics
GSM 02.19	SIM Application Programming Interface (SIM API)
GSM 02.22	Personalization of GSM Mobile Equipment (ME)

GSM 02.30	Man Machine Interface of the Mobile Station
GSM 02.48	Security mechanisms for the SIM Application Toolkit - Stage 1
GSM 03.19	Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™
GSM 03.20	Security Related Network Functions
GSM 03.38	Alphabets and language-specific information
GSM 03.40	Short Message Service
GSM 03.48	Security Mechanisms for the SIM Application Toolkit - Stage 2
GSM 11.11	Specification of the SIM/ME Interface
GSM 11.12	Specification of 3V SIM/ME Interface
GSM 11.14	Specification of SIM Application Toolkit
GSM 11.17	Subscriber Identity Module (SIM) test specification
GSM 11.18	(Reserved for 1.9V SIM)
GSM 11.10	Mobile Station Conformity Specification
GSM 11.40	System Simulator Specification

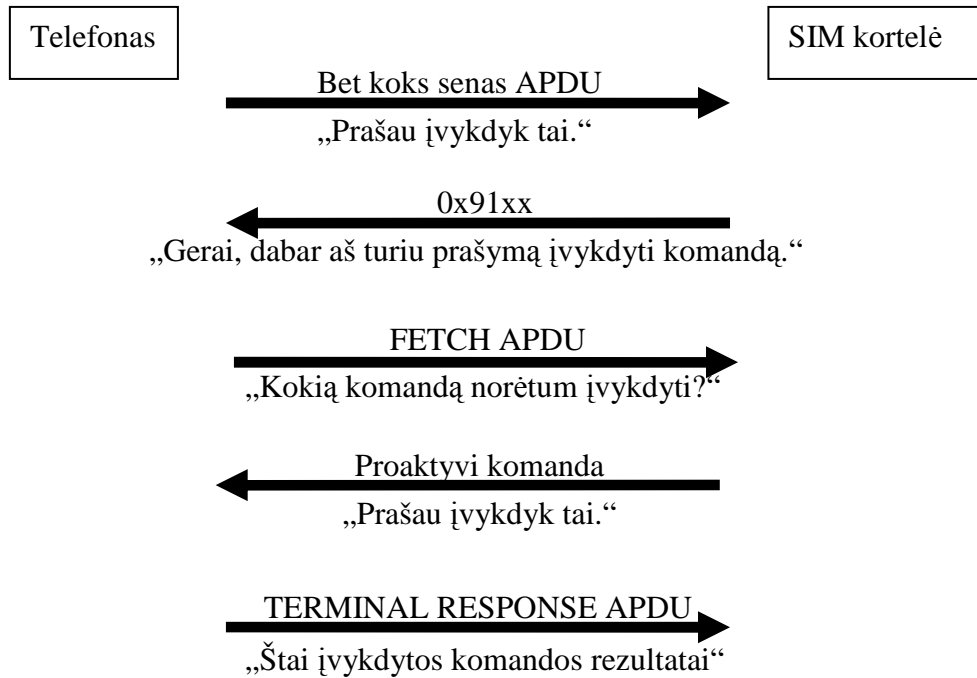
2 lentelė. SIM kortelių standartai

1.2. SIM įrankinių rinkinys – SAT

SIM įrankių rinkinys (angl. SIM Application Toolkit) – SAT – leidžia SIM kortelei tiesiogiai kreiptis pasiekti mobiliojo įrenginio funkcijas, pavyzdžiui, parodyti tekstą ekrane, paleisti telefono WAP naršyklę, užmegzti dialogą su vartotoju, perimti skambučio kontrolę ir kt., kurių pagalba atsiranda galimybė kurti pridėtinės vertės (angl. value-added) paslaugas. Kitaip tariant, SAT yra konstravimo įrankis, kuris leidžia beveik bet kokią taikomąją programą realizuoti SIM kortelėje [RE04].

1.2.1. Proaktyviosios komandos

Proaktyvi komanda – tai komanda, kurią SIM kortelė siunčia telefonui, „prašydama“ tą komandą atlikti. Komanda vadinama proaktyvia todėl, kad iš tiesų ne telefonas, o SIM kortelė yra komandos iniciatorius, tačiau iš kitos pusės, pati SIM kortelė komandų inicijuoti negali ir minėti „prašymai“ įvykdyti vieną ar kitą komandą yra pateikiami atsakyme į prieš tai telefono inicijuotą komandą. Schematiškai proaktyvios komandos įvykdymas yra pavaizduotas 4 pav.



4 paveikslas. Proaktyvios komandos įvykdymas

Proaktyvios komandos skirstomos į tokias kategorijas [GC02]:

- Taikomųjų programų komandos – naudojamos kuriant tipines SIM Toolkit programas;
- Intelektualiosios kortelės komandos – naudojamos bendravimui su kita intelektualiąja kortele, prijungta prie įrenginio;
- Bendros komunikavimo komandos – bendros paskirties interfeisas priėjimui prie duomenų pernešėjų, kuriuos palaiko telefonas;
- Sisteminės komandos – naudojamos sinchronizacijai su telefonu ir tinklu.

3 lentelėje yra išvardintos visos proaktyvios komandos, jų paskirtis ir nuoroda į [GSM 11.14] sekciją, kurioje konkreti komanda yra aprašyta.

Komanda	Paskirtis	Nuoroda GSM 11.14 standarte
DISPLAY TEXT	Atvaizduoti tekstą	Sekcija 6.4.1
GET INKEY	Nuskaityti vartotojo įvestį	Sekcija 6.4.2
GET INPUT	Nuskaityti vartotojo įvestį	Sekcija 6.4.3
LAUNCH BROWSER	Paleisti įrenginio naršyklę	Sekcija 6.4.26

PLAY TONE	Groti garsą	Sekcija 6.4.5
REFRESH	Atnaujinti	Sekcija 6.4.7
SELECT ITEM	Atvaizduoti meniu	Sekcija 6.4.9
SEND SHORT MESSAGE	Siųsti SMS žinutę	Sekcija 6.4.10
SEND SS	Siųsti SS žinutę	Sekcija 6.4.11
SEND USSD	Siųsti USSD žinutę	Sekcija 6.4.12
SET UP CALL	Užmegzti skambutį	Sekcija 6.4.13
SET UP EVENT LIST	Nustatyti įvykių sąrašą	Sekcija 6.4.16
SET UP IDLE MODE TEXT	Nustatyti budėjimo režimo tekstą	Sekcija 6.4.22
SET UP MENU	Atvaizduoti meniu	Sekcija 6.4.8
CLOSE CHANNEL	Uždaryti kanalą	Sekcija 6.4.28
GET CHANNEL STATUS	Gauti kanalo būseną	Sekcija 6.4.31
GET READER STATUS	Gauti skaitytuvo būseną	Sekcija 6.4.20
LANGUAGE NOTIFICATION	Kalbos notifikacija	Sekcija 6.4.25
MORE TIME	Prašyti daugiau laiko	Sekcija 6.4.4
OPEN CHANNEL	Atidaryti kanalą	Sekcija 6.4.27
PERFORM CARD APDU	Siųsti APDU papildomai kortelei	Sekcija 6.4.17
POLL INTERVAL	Apklausimo intervalas	Sekcija 6.4.6
POLLING OFF	Apklausimo išjungimas	Sekcija 6.4.14
POWER OFF CARD	Atjungti papildomą kortelę	Sekcija 6.4.18
POWER ON CARD	Ijungti papildomą kortelę	Sekcija 6.4.19
PROVIDE LOCAL INFORMATION	Pateikti vietinę tinklo informaciją	Sekcija 6.4.15
RECEIVE DATA	Gauti duomenis iš kanalo	Sekcija 6.4.29
RUN AT COMMAND	Vykdyti AT komandą	Sekcija 6.4.23
SEND DATA	Siųsti duomenis kanalu	Sekcija 6.4.30
SEND DTMF	Siųsti DTMF tonus	Sekcija 6.4.24

TIMER MANAGEMENT	Taimerio valdymas	Sekcija 6.4.21
------------------	-------------------	----------------

3 lentelė. Proaktyvios komandos

1.2.2. Prenumeruojami įvykiai

SET UP EVENT LIST komandos pagalba SAT programa gali prenumeruoti įvykius, įvykstančius telefone. Tokių įvykių pavyzdžiai gali būti gauta SMS žinutė², SAT meniu punkto pasirinkimas, įeinančio arba išeinančio skambučio užmezgimas ir kt. Pilnas tokių įvykių sąrašas yra pateiktas 4 lentelėje.

Pavadinimas	Paskirtis
SMS-PP	Gauta formatuota SMS žinutė
CELL BROADCAST	Gauta tinklo paslaugos žinutė
MENU SELECTION	Pagrindiniame SIM meniu buvo atliktas meniu punkto pasirinkimas
CALL CONTROL	Vartotojas bando užmegzti skambutį
SMS CONTROL	Vartotojas siunčia SMS žinutę
TIMER EXPIRATION	Vienas iš prenumeruojamų taimerių baigėsi
MT CALL	Gautas įeinantis balso skambutis
CALL CONNECTED	Jungiamas balso skambutis
CALL DISCONNECTED	Atjungiamas balso skambutis
LOCATION STATUS	Geografinės vietos pasikeitimas
USER ACTIVITY	Telefono klavišo paspaudimas
IDLE SCREEN AVAILABLE	Ekranas šiuo metu yra budėjimo režime
CARD READER STATUS	Įvyko įvykis išorinėje intelektualiojoje kortelėje
LANGUAGE SELECTION	Vartotojas pasikeitė telefono kalbą
BROWSER TERMINATION	Telefono naršyklė buvo išjungta
DATA AVAILABLE	Viename iš duomenų kanalų atsirado duomenų
CHANNEL STATUS	Pasikeitė vieno iš duomenų kanalo būseną
ACCESS TECHNOLOGY CHANGE	Prisijungimas prie kito tarptinklinio ryšio operatoriaus
DISPLAY PARAMETERS CHANGED	Vartotojas pakeitė ekrano parametrus

4 lentelė. SAT taikomosios programos prenumeruojami įvykiai

² SMS žinutė gali būti įprasta neformatuota arba formatuota, skirta konkrečiai SAT taikomajai programai.

1.3. Java kortelė – Java Card

Java Card – tai kompanijos Sun Microsystems kartu su Java Card forumu ir stambiaisiais intelektualųjų kortelių gamintojais sukurtas standartų rinkinys, apibrėžiantis Java kalbos poaibį intelektualiosiose kortelėse, tarp kurių ir SIM kortelėje. Išskiriami šie pagrindiniai Java Card privalumai [WIT01]:

- Suderinamumas (angl. interoperable) – verifikuotos Java Card programos - apletai veikia bet kurioje Java Card kortelėje;
- Multiprogramiškumas (angl. multi-application) – vienu metu gali dirbti keli apletai
- Dinamiškumas (angl. dynamic) – nauji apletai gali būti pridėti jau po kortelės išdavimo vartotojui;
- Saugumas (angl. secure) – Java saugumo mechanizmai yra paveldimi ir praplečiami tam tikrais apribojimais.

Java Card specifikacija gana stipriai apriboja tradicines Java galimybes. Java Card apletuose draudžiama (iki 2.2 versijos) dinamiškai kurti naujus objektus, tame tarpe ir masyvus, kadangi nėra šiukšlių surinkėjo (angl. garbage collector). Pagrindinis duomenų apsikėitimas vyksta statinių baitų masyvų pagalba, kuriems irgi iš anksto turi būti išskirta atmintis.

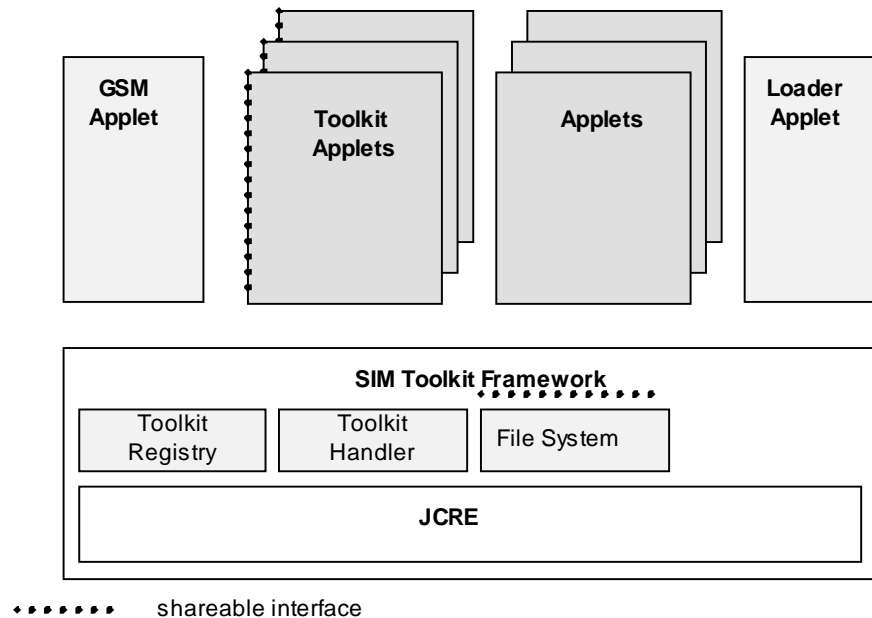
Java Card realizacija SIM kortelėse įgalina pasiekti funkcijas ir duomenis [GSM 11.11] ir [GSM 11.14] Java programavimo kalba. Java Card architektūra SIM kortelėje yra pavaizduota 5 pav. [GSM 03.19] standartas numato apribojimus, kurie galioja SIM kortelėje veikiantiems apletams bei apibrėžia API (programuotojo sąsają), kuri yra specifinė SIM servisams. Kaip matyti iš 5 pav., SIM kortelėje gali veikti tiek įprasti apletai, tiek *Toolkit* tipo³. Pastariesiems būdinga savybė, kad juos gali aktyvuoti kortelės menedžeris (Card Manager) per *processToolkit* metodą.

[GSM 03.19] numato keturis laikinuosius Java Card vykdymo aplinkos objektus (Temporary JCRE Entry Point Object), kurių pagalba apletas gali siųsti komandas SIM kortelei ar telefonui:

- ProactiveHandler – proaktyvios komandos formavimui;
- ProactiveResponseHandler – atsako gavimui į įvykdytą proaktyvią komandą;

³ T.y. tie, kurie realizuoja *ToolkitInterface* interfeisą.

- EnvelopeHandler – *ENVELOPE* komandos duomenų nuskaitymui;
- EnvelopeResponseHandler – atsako į *ENVELOPE* komandą formavimui.



5 paveikslas. Java Card architektūra SIM kortelėje [GSM 03.19]

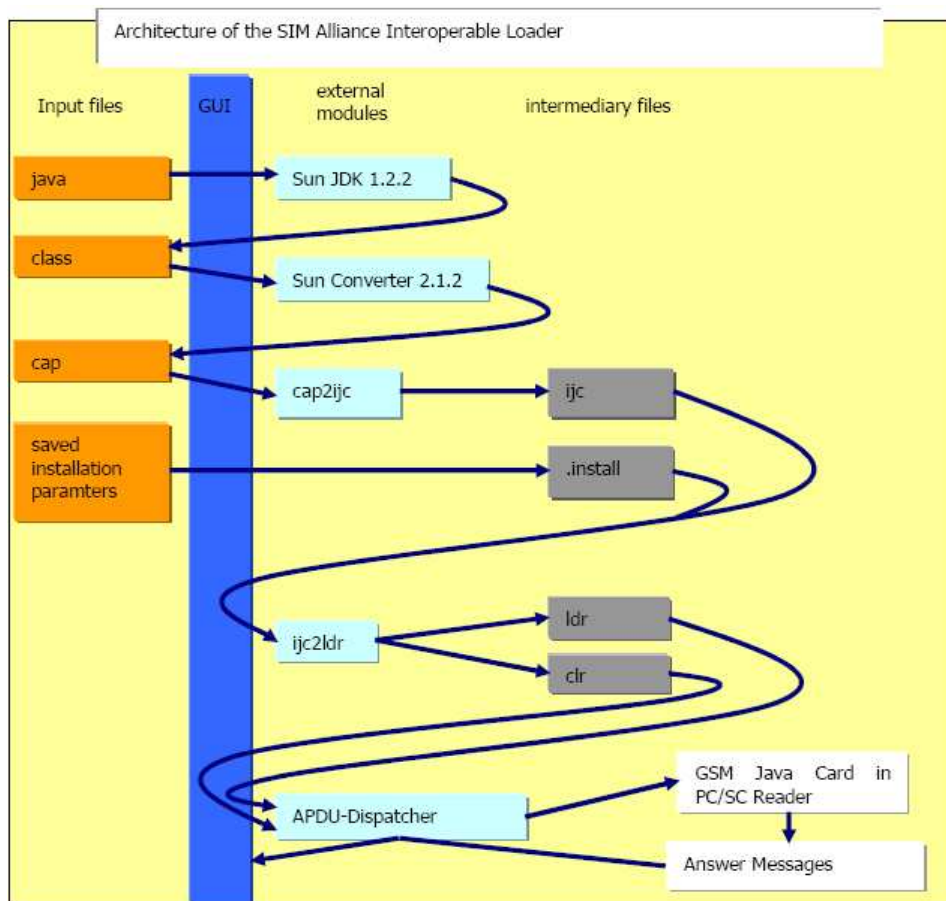
Du apletai tarpusavyje gali bendrauti, t.y. apsikeisti duomenimis per *Shareable* interfeisą. Apletai SIM kortelėje yra vienareikšmiškai identifikuojami taikomosios programos identifikatoriumi AID.

Java Card apleto įdiegimas susideda iš kelėtos dalių. Visų pirma apletas turi būti validus Java kodas, t.y. atitikti Java Card specifikaciją, [GSM 03.19], [GSM 11.11] ir [GSM 11.14] standartus. Vėliau išėities tekstas yra transliuojamas į Java baitų kodą (angl. bytecode) – gauname CLASS failą, kuris yra optimizuojamas ir sutransliuojamas į CAP (angl. Cardlet Package) failą. Pastarasis yra dar kartą transformuojamas į komandas, kuriomis apletas jau gali būti užkrautas į SIM kortelę. 6 pav. yra pavaizduotas Java Card kūrimo ir užkrovimo į SIM kortelę procesas.

[IIO06] rekomenduoja, kad, dėl didesnio suderinamumo, apleto Java kodas būtų kompiliuojamas naudojant JDK (angl. Java Development Toolkit) 1.4.1 versiją. Iš CLASS failo gauti CAP failą galima naudojantis konvertavimo įrankiu, pateikiamu prie Sun Microsystems platinamo Java Card įrankių rinkinio JCDK. ICJ (angl. Interoperable Java CAP file) gaunamas naudojantis SIM aljanso įrankiu *cap2icj*, kurio pagalba taip pat

gaunamas LDR failas⁴, o CLR faile yra įrašomos komandos, reikalingos apieto demontavimui.

Pastebėsime, kad naudojantis komerciniais SIM kortelių gamintojų įrankiais, pavyzdžiui, Axalto [VIEWS] Professional, minėtas procesas yra integruojamas į vieningą vartotojo sąsają, tačiau paprastai yra pritaikytas tik programų įdiegimui į pačio gamintojo gaminamas SIM korteles. Svarbu paminėti ir kitą Java Card iniciatyvą – tai IBM JCOP projektas, kuris už simbolinę platina Java Card kūrimo priedą populiariai programuotojo aplinkai Eclipse. Tiesa, naujausioje – JCOP Tools 3.0 – versijoje nebeliko apietų SIM kortelėje kūrimui reikalingų priedų.



6 paveikslas. Java Card kūrimo ir užkrovimo į SIM kortelę procesas [ISS06]

1.4. SIM valdymas nuotoliniu būdu – OTA

Po to, kai SIM kortelė yra išduodama mobiliojo ryšio operatoriaus klientui, neretai yra reikalinga užmėgsti tiesioginį ryšį su SIM kortele esamų taikomųjų programų valdymui ir naujų paslaugų sukūrimui. Tam tikslui [GSM 03.48] standartas pateikia mechanizmus, kurių

⁴ Žinutė su Open Platform komandomis, tenkinanti [GSM 03.48] reikalavimus.

pagalba išorinei sistemai galima saugiai užmegzti tiesioginį ryšį su SIM kortele. Toks komunikacijos mechanizmas vadinamas OTA. Bendra OTA architektūra yra pavaizduota 7 pav.

Kadangi poreikis tokiai komunikacijai atsirado jau įsibėgėjus GSM technologijų plėtrai, komunikavimui su SIM kortele teko panaudoti egzistuojančius duomenų pernešėjus. Šiuo atveju pagrindiniu komunikavimo kanalu buvo pasirinktos trumposios SMS žinutės. Egzistuoja ir kiti galimi pernešėjai – tinklo paslaugos žinutės (angl. cell broadcast) bei nuo pernešėjo nepriklausantis protokolas BIP, tačiau jų šiame darbe plačiau nenagrinėsime.

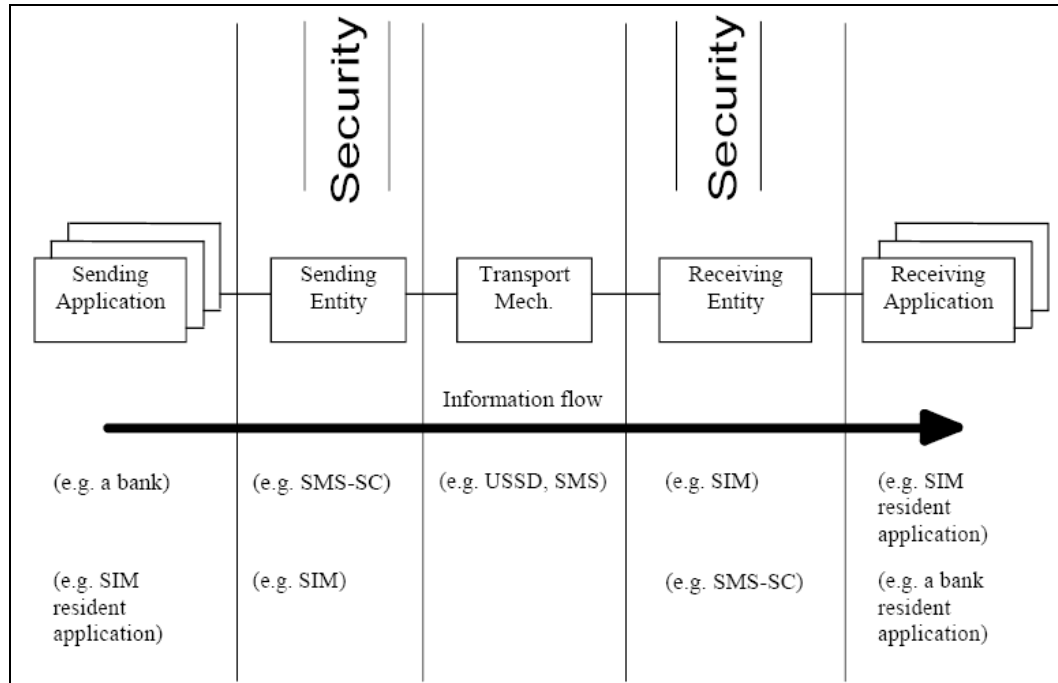
OTA saugaus komunikavimo standartas [GSM 03.48] pateikia platų spektrą persiunčiamų duomenų apsaugojimo mechanizmų. Paprasčiausias iš jų – naudojant ciklinės dubliavimo schemos CRC (angl. Cyclic Reduncancy Scheme) santrauką (angl. checksum) duomenų apsaugojimui nuo galimų persiuntimo klaidų. Kalbant apie kriptografinę apsaugą, kartu su duomenimis yra naudojamas siuntimo sekos skaitliukas, o patys duomenys gali būti šifruojami DES arba trigubu (su vienu arba dviem raktais) DES algoritmu. Jeigu reikalinga, papildomai gali būti paskaičiuojama duomenų santrauka MAC arba skaitmeninis parašas.

Aprašysime OTA komunikavimo veikimo principą kaip duomenų nešėją naudojant SMS žinutes. Pavyzdžiui, jeigu išorinė sistema nori pasiųsti komandą konkrečiai SIM kortelei, ji sugeneruoja trumpąją žinutę su norima komanda, papildomai žinutę apsaugant kriptografiniais saugumo mechanizmais. Iš karto po to, kai telefonas, kuriame yra SIM, įjungiamas, žinutė yra persiunčiama signalizavimo kanalu. Remiantis žinutės kodavimu kaip nurodyta GSM 03.40, telefonas atpažįsta, kad žinutėje yra SIM kortelei skirti duomenys ir naudoja *SAT ENVELOPE* komandą persiųsti žinutę SIM, kuri interpretuoja gautą žinutę, atsirenka gautą komandą ir ją įvykdo. Papildomai, SIM kaip atsaką į komandą ar jų rinkinį irgi gali generuoti SMS žinutę. Tokiu atveju ji būtų persiunčiama kaip atsakas į *FETCH* komandą, o mobilus įrenginys ją tinklu persiustų į išorinę sistemą.

Aprašyto mechanizmo pagalba galima užmegzti abipusį ryšį tarp išorinės sistemos ir SIM kortelės, kuris yra nematomas tarpiniams komponentams, tame tarpe ir mobiliojo ryšio vartotojui. Toks komunikavimo kanalas gali būti naudojamas duomenų keitimui failuose (pavyzdžiui, pasikeitus operatoriaus pavadinimui ar atsiradus naujam tarptinklinio ryšio partneriui) kaip išorinio failų valdymo RFM dalis. OTA taip pat gali būti panaudojama sudėtingesniems uždaviniams, pavyzdžiui, naudo Java Card apleto atsiuntimui ir instaliavimui į SIM kortelę.

Deja, [GSM 03.48] ne visos dalys yra tiksliai specifikuotos ir dėl šios priežasties daugelis SIM kortelių gamintojų naudoja uždarus (angl. proprietary) komunikavimo mechanizmus,

kurie atitinka jų poreikius. Dėl šios priežasties atsirado daugybė problemų dėl skirtingų gamintojų SIM kortelių suderinamumo.



7 paveikslas. OTA sistemos architektūra [GSM 03.48]

1.4.1. Nuotolinis failų valdymas – RFM

RFM – tai failų SIM kortelėje valdymas naudojant OTA mechanizmus. Jį apibrėžia [GSM 03.48] standartas pagal reikalavimus iš GSM 02.48 standarto.

Tik nedaugelis SIM [GSM 11.14] apibrėžtų komandų gali būti naudojamos nuotoliniam failų valdymui, tačiau duoto poaibio paprastai pakanka norimiems rezultatams pasiekti. Pastarasis poaibis yra dalinamas į dvi dalis: įėjties (angl. input) komandas, kuriomis duomenys yra siunčiami SIM ir išėjties (angl. output) komandas, kurios prašo duomenų iš SIM. Išorinė sistema vienoje OTA žinutėje gali siųsti ne viena komandą, o visą jų seką, tačiau komandų sąrašui galioja apribojimas – tik paskutinė sąrašo komanda gali prašyti duomenų iš SIM. 5 lentelėje yra pateiktos įėjties ir išėjties komandos, leidžiamos naudoti RAM.

Įėjties komandos	Išėjties komandos
SELECT, UPDATE BINARY, UPDATE RECORD, SEEK, INCREASE, VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV, UNBLOCK CHV, INVALIDATE	READ BINARY, READ RECORD GET RESPONSE

REHABILITATE	
--------------	--

5 lentelė. RAM naudojamos įeities ir išeities komandos

Pateiksime RAM, kaip duomenų kanalą naudojant, pavyzdį [RE04]. Jeigu išorinė sistema nori keisti konkretų numerį SIM adresų knygelėje, kuri saugoma elementariajame faile EF ADN, turi būti atlikti tokie veiksmai. Pirmoje OTA žinutėje⁵ aktyvioju (komanda *SELECT*) yra padaromas EF ADN failas, prieš tai parenkant DF TELECOM katalogą (nes ADN failas priklauso katalogui TELECOM). Paskutinė OTA žinutės komanda turi būti *READ RECORD* su nurodytu įrašo numeriu, kuris yra žinomas išorinei sistemai. Pastarosios komandos įvykdymo metu bus nuskaitytas norimas įrašas ir rezultatas (duomenys) gražinamas kaip atsakas SMS žinute per OTA. Jeigu gautas rezultatas nesutampa su tuo, ko išorinė sistema tikėjosi, siunčiama OTA žinutė su komanda *UPDATE RECORD*, taip perrašant seną įrašą nauja reikšme.

Svarbu pastebėti, kad kai kurių failų modifikavimas gali sukelti problemų stabiliam telefono darbui. Pavyzdžiui, EF SST (SIM Service Table) yra saugomos aktyvios SIM kortelės paslaugos, todėl deaktyvavus vieną iš jų, gali perkauti telefoną ir pan.

SIM kortelėje taip pat yra du failai, kuriuos draudžiama modifikuoti. Tai EF ICCID, kuriame yra saugomas SIM kortelės identifikacinis numeris ir EF KC, kuris saugo raktą, naudojamą duomenų kodavimui tarp telefono ir bazinės stoties.

1.4.2. Nuotolinis taikomųjų programų valdymas – RAM

[GSM 03.48] specifikacija taip pat aprašo nuotolinį taikomųjų programų valdymą RAM, kuris nedaug skiriasi nuo RFM. Nuotolinis taikomųjų programų valdymas leidžia valdyti Java Card apletus naudojant tiesioginį ryšį tarp išorinės sistemos ir SIM kortelės.

Pagrindinis reikalavimas RFM yra SIM kortelės suderinamumas su [GSM 03.19] standartu, kuris paremtas Java Card (2.1 ar 2.2) specifikacijomis. Visos apletų valdymo komandos yra paremtos Open Platform specifikacija.

Į taikomųjų programų valdymą įeina komandos, skirtos SIM kortelėje esančių Java apletų užkrovimui, instaliavimui, šalinimui, užrakinimui ir atrakinimui. Panašūs mechanizmai yra skirti Java paketų kūrimui ir šalinimui iš SIM.

⁵ OTA žinutę gali sudaryti ir žinučių seka, naudojant ilgąsias – jungtines SMS žinutes.

Kaip ir RFM atveju, dažniausiai RAM duomenų perdavimui per OTA yra naudojamos SMS žinutės. Čia galioja tokios pačios taisyklės ir saugumo mechanizmai, kaip ir nuotoliniame failų valdyme.

Taip pat labai svarbu pastebėti, kad lyginant su RFM, RAM turi dar daugiau suderinamumo problemų tarp skirtingų gamintojų SIM kortelių. Dėl šios priežasties SIM aljansas kartu su didžiausiais gamintojais išleido rekomendacijų rinkinį [ISS06], numatantį bendras apletų kūrimo ir valdymo taisykles, kurių turi laikytis visi aljanso nariai.

2. Esamų STK programų problemų apžvalga

Java Card platforma yra naudojama įvairiose taikomosiose srityse – bankininkystės, biometrijos, asmens duomenų identifikavimo, telekomunikacijų ir nemažai kitų. SIM modulis – tai populiariausia intelektualioji kortelė, kurioje taip pat yra naudojama Java Card technologija. Taikomųjų programų kūrimą SIM kortelėje su Java Card platforma apriboja ne tik Java Card specifikacijų rinkinys [JCSPEC], tačiau ir visa eilė GSM standartų. Būtent pastaroji priežastis sąlygoja gana komplikuoatą nors ir elementarios Java Card programos – apleto – įdiegimą į SIM modulį. Visų pirma, tai – itin griežti saugumo reikalavimai, kuriuos mobilaus ryšio operatorius yra priverstas taikyti ryšio paslaugų vartotojams išduodamas korteles. Bet kokia saugumo spraga gali sukelti neteisėtą pasinaudojimą mobilaus ryšio paslaugomis, apsimetimą kitu ryšio vartotoju ir nemažai kitų problemų.

Taip pat reikia pastebėti, kad skirtingi ryšio operatoriai naudoja skirtingų intelektualųjų kortelių gamintojų SIM modulius (dažna praktika kaip tiekėjus yra pasirinkti kelis gamintojus). Tai lemia, kad mobiliojo ryšio operatoriui ar jo partneriui norint savarankiškai, t.y. be SIM kortelių gamintojo pagalbos, įdiegti taikomąją STK programą į išduodamas SIM korteles gali pareikalauti nemažai laiko bei investicinių resursų. Nėgana to, norint, kad įdiegta STK programa galėtų su išoriniu pasauliu keistis duomenimis, reikalingas papildomas elementas operatoriaus infrastruktūroje – OTA platforma, kuri būtų suderinama su naudojamomis SIM kortelėmis. Nors egzistuoja nemažai komercinių sprendimų, kurie siūlo įvairialypes OTA platformas⁶, tačiau dažniausia realus tokios platformos funkcijų poreikis skiriasi nuo to, kurį siūlo gamintojai.

Griežti saugumo reikalavimai bei susitarimai dėl standartų taip pat yra vienas pagrindinių faktorių, lemiančių mobiliojo elektroninio parašo problematiką. Nors atrodytų, jog esamos technologijos leidžia realizuoti mobiliąją viešojo rakto infrastruktūrą, realybėje susiduriama su visa eile problemų, visų pirma – specifika, būdinga SIM kortelėse veikiančioms taikomosioms programoms, jų bendravimu su išorinėmis sistemomis, ribota vartotojo sąsaja ir kt.

Šio darbo metu kuriant StartDial projektą, visų pirma buvo susidurta su literatūros, kuri aprašytų priemones, reikalingas paprasčiausią Java Card apletą įdiegti į testavimui paruoštą SIM kortelę⁷, trūkumu. Tas pats galioja ir pačioms priemonėms – integruotoms programuotojo aplinkoms, kurios beveik visais atvejais yra mokamos ir pritaikytos dirbti su konkretais SIM kortelių gamintojų SIM moduliais. Verta paminėti ir tai, kad ne taip jau

⁶ Pavyzdžiui, SmartTrust produktų rinkinys [SMTRUST].

⁷ Testavimui paruoštuose SIM kortelėse paprastai atsisakoma simetrinių raktų

paprasta rasti taip vadinamą „Hello World“⁸ atitikmenį STK programos, kadangi vien apleto Java kodo šiuo atveju nepakanka. Reikalinga išsiaiškinti ir visus kitus žingsnius, kuriuos būtina atlikti norint realiai pamatyti programos elgseną.

Kita problema – tai ne visiškai standartų atitikimas realybėje bei tai, kad skirtingi mobilūs įrenginiai skirtingai interpretuoja ir reaguoja į [GSM 11.14] komandas. Taip pat paaiškėjo, kad norint OTA sinchronizacijai naudoti sujungtas (angl. concatenated) žinutes, reikalinga atitinkama konfigūracija SIM kortelėje, nors standartuose tai nenumatyta.

Ribotos ir STK programų testavimo galimybės. Visų pirma, ne visada testavimas simulatoriaus pagalba duoda tuos pačius rezultatus, kokie jie būna testuojant su realiu mobiliuoju įrenginiu. Dar daugiau, neretai skirtingus rezultatai gaunami net ir tą pačią STK programą testuojant su skirtingais įrenginiais, todėl prieš išleidžiant produktą į rinką, būtinas testavimas su įvairių gamintojų ir modelių telefonais.

⁸ „Labas, Pasauli“ – taip vadinamos pavyzdinės, paprastos, tačiau realiai veikiančios programos.

3. StartDial projektas

Šiame skyriuje pristatysime pavyzdinį STK projektą StartDial, aptarsime jo reikalingumą, keliamus techninius reikalavimus, pateiksime galimą modelių analizę, StartDial programos savybes, architektūrą, realizacijos ypatumus bei bendravimą su išorinėmis sistemomis naudojantis OTA mechanizmais. Skyriaus pabaigoje yra pateikiami testavimo rezultatai, o taip pat papildomos savybėmis, kuriomis būtų galima išplėsti StartDial.

3.1. StartDial reikalingumas

Nepaisant to, kad sparčiai didėja vartotojų, naršančių mobilaus interneto svetaines mobiliųjų telefonų pagalba, tam tikras mobilusis turinys ir paslaugos vis dar yra sunkiai pasiekiami telefonų naudotojams. Viena to priežasčių – telefonų dizainas. Mobilaus telefono paskirtis visų pirma yra užmegzti skambutį, bet ne įvedinėti internetinius adresus. Daugelis vartotojų mobiliųjų internetą pasiekia per taip vadinamą ryšio operatoriaus „namų puslapį“ ir jame esančias nuorodas, ir tik maža dalis tiesiogiai, įvesdami konkretų URL adresą.

Paprastai vartotojui yra reikalinga praleisti nemažai laiko tam, kad patektų į savo norimą svetainę. Arba tai yra daroma įsimintų adresų (angl. bookmarks) pagalba, arba įvedant pilną svetainės adresą mobiliuoju telefonu. Abiem atvejais procesas užtrunka vidutiniškai nuo 10 sekundžių iki minutės ar daugiau.

StartDial projekto pagrindinė idėja ir buvo išspręsti minėtą problemą – pakankamai komplikotą patekimą į tam tikrą interneto svetainę. Pasinaudojant StartDial programa pakanka surinkti tam tikrą skaičių kombinaciją (pvz. *123) ir paspausti skambinimo mygtuką. Šis skambutis bus perimtas StartDial programos ir vietoj įprastinio skambučio užmezgimo bus paleista telefono WAP naršyklė su dinamiškai nustatytu URL, atitinkančiu numerį, kuriuo „skambinama“. Visa tai atliekama be didesnių užlaikymų.

Tam, kad atskirti, ar „skambinamas“ numeris yra įprastinis fiksuoto ar mobilaus ryšio numeris, ar StartDial trumpinys, įvedamas pasirinktas prefiksas (pvz. * simbolis). Tokiu būdu turint dviženklį trumpinį galima apibrėžti 100 skirtingų kiekvieną trumpinį atitinkančių URL adresų (esant triženkliam trumpiniui – 1000 adresų ir t.t.).

Kadangi StartDial trumpinys beveik niekuo nesiskiria nuo įprastinio telefono numerio, telefono vartotojui atsiranda galimybė trumpinius saugoti telefono adresų knygelėje, juos persiųsti SMS žinute kaip vizitinę kortelę ir pan.

Kiekvienas trumpinį atitinkantis URL gali būti susiejamas su paslaugų tiekėjo – mobilaus turinio partnerio – svetaine. Žiniatinkliu paremtos administravimo sąsajos pagalba

patys partneriai galėtų susieti trumpinius su URL adresais, o tokia susiejimų duomenų bazė būtų nusiųsta į mobilaus ryšio naudotojų SIM korteles.

StartDial panaudojimo galimybės neapribotos vien mobilaus interneto svetainių pasiekiamumu. Skambinimas tam tikrais trumpiniais gali iššaukti įvairių paties mobilaus ryšio operatoriaus siūlomų paslaugų (pavyzdžiui, paskutinių skambučių išklotinės) peržiūra, elektroninio bilieto pirkimo proceso inicijavimą, balsavimą ir pan.

3.2. Techniniai reikalavimai

Techniškai StartDial sprendimas yra tinkamas mobiliojo ryšio 2.5G/3G aplinkoje (kartoje), kur yra naudojamos pranašesnės mobilaus interneto bei duomenų paslaugos, o didžioji dauguma telefonų turi integruotas WAP (taip pat ir WWW) naršykles. Išskirsime tris pagrindinius reikalavimus pilnam StartDial funkcionavimui:

- Kritinė mobiliojo ryšio paslaugų vartotojų dalis turėtų turėti su Java Card specifikacijomis suderintą SIM kortelę, kurioje būtų įdiegta StartDial programinė įranga (arba turėti galimybę ją įdiegti OTA atnaujinimų pagalba);
- Norint, kad StartDial pasiektų kritinę masę vartotojų, reikalinga, kad sprendimas galėtų veikti visuose didžiųjų mobilaus ryšio operatorių SIM kortelėse;
- Paslaugos naudotojo WAP/WWW naršyklė turi būti tinkamai nustatyta. Galima paminėti, kad StartDial pagalba yra galimybė ryšio operatoriui pranešti apie nesėkmingus naršyklės paleidimus. Tokiu atveju vartotojas naršyklės nustatymus galėtų gauti OTA pagalba.

Viena pagrindinių StartDial, kaip ir kitų STK taikomųjų programų problema yra programinės įrangos įkrovimas į egzistuojančias arba diegimas į naujas SIM korteles. Svarbu pastebėti, kad StartDial sprendimas nereikalauja SIM kortelės (su sąlyga, kad ji suderinama su Java Card specifikacijomis) keitimo, kadangi kaip ir kitas STK programas, ją galima įdiegti naudojant OTA mechanizmus. Techniškai taip pat yra įmanomas StartDial paruošimas su Java Card platforma nesuderintai SIM operacinei sistemai (pvz. MultOS), tačiau toks nagrinėjimas reikalautų atskiros studijos.

3.3. Galimų modelių analizė

Išanalizavus galimus architektūros modelius, išskirsime du galimus sprendimus realizuoti StartDial projektą. Pirmajame modelyje biznio logika yra sukoncentruota serverio pusėje, o antrajame beveik viskas atliekama SIM kortelėje, serverinę dalį (angl. backend) naudojant tik kaip duomenų saugyklą. Toliau panagrinėsime kiekvieno iš modelio privalumus bei trūkumus.

3.3.1. Serverine dalimi paremtas sprendimas

Esant šiam sprendimui, Java Card apletas tampa palyginti nežymiu komponentu visoje infrastruktūroje. Duomenų bazės valdymas yra deleguotas serverinei daliai, todėl nėra jokios prasmės duomenis papildomai saugoti SIM kortelėje. Šis sprendimas taip pat nereikalauja OTA sinchronizacijos. Kiekvieną kartą vartotojui bandant „skambinti“ tam tikru trumpiniu, įvykdoma LAUNCH BROWSER komanda, URL visuomet nurodant centrinio serverio ir tik per HTTP GET parametrą perduodant surinktą trumpinį. Tuomet realaus URL paiešką duomenų bazėje bei vartotojo nukreipimą į rastą URL, atitinkantį rinktą trumpinį, yra serverio užduotis.

Kiti serverine dalimi paremto sprendimo privalumai yra galimybė fiksuoti vartotojo veiksmus, pateikti statistinę informaciją bei kaupti papildomą informaciją, tokią kaip vartotojo buvimo vietą tuo metu, kai buvo renkamas trumpinys.

Nors taikant šį sprendimą nauji trumpiniai tampa pasiekiami iš karto po to, kai jie yra įvedami į centrinę duomenų bazę, šis sprendimas taip pat turi keletą trūkumų. Visų pirma, žiniatinklo serveris turi veikti nepertraukiamai 24 valandas per parą, o tai reiškia, kad jis tampa kritiniu veikimo tašku SPF (angl. Single Point of Failure). Kita problema pasireiškia tuomet, kai vartotojas įveda neegzistuojantį trumpinį. Tokiu atveju ME naršyklė yra vis tiek bus paleidžiama, o serverinė dalis, neradusi trumpinį atitinkančio URL, suformuos klaidos pranešimą. Šitaip bus ne tik eikvojami telefono resursai bei GPRS ryšys, bet ir dažnai neatitiks vartotojo lūkesčių, kadangi klaidos pranešimo pavaizdavimas gali užtrukti iki 10 sekundžių.

3.3.2. SIM kortele paremtas sprendimas

Taikant šį sprendimą, beveik visa biznio logika yra sukoncentruota Java Card aplete, kuris veikia SIM kortelėje. Nors šis sprendimas nėra trivialus, jis turi kelis svarbius privalumus. Visų pirma, duomenis saugant vidinėje SIM kortelės atmintyje tampa įmanoma

įgyvendinti papildomas funkcijas, tokias kaip automatinis trumpinio papildymas, t.y. įvedus trumpinio pradžia, būtų parodomi visi taip prasidedantys trumpiniai bei juos atitinkantys URL. Turint visą reikalingą informaciją telefone, atsiranda galimybė pateikti daugiau informacijos apie konkretų trumpinį – vartotojui parodyti jo aprašymą bei URL tiek interaktyviame režime, tiek kitose programos panaudojimo vietose. Manome, kad tai yra svarbus interfeiso privalumas.

Nors šiam, SIM kortele paremtam sprendimui realizuoti yra būtina sukurti OTA sinchronizacijos mechanizmus, šiame darbe buvo pasirinktas būtent šis sprendimas, siekiant geriau pažinti pačią technologiją bei sukurti vartotojui labiau draugišką sąsają.

Nepaisant to, sukūrus apletą, kuris kaip duomenų bazę naudotų SIM elementarų failą, tampa nesudėtinga pereiti prie serverine dalimi paremto sprendimo ir taip įgyvendinti naudojamumo stebėjimo bei kitas funkcijas. Kitas variantas yra abiejų sprendimų rinkinys, kuomet visi duomenys galėtų būti saugomi SIM kortelėje, tačiau visi LAUNCH BROWSER paleidimai pasiektų viena centrinę tašką – HTTP tarpinę grandį (angl. proxy), kuri atliktų naudojamumo fiksavimo funkcijas.

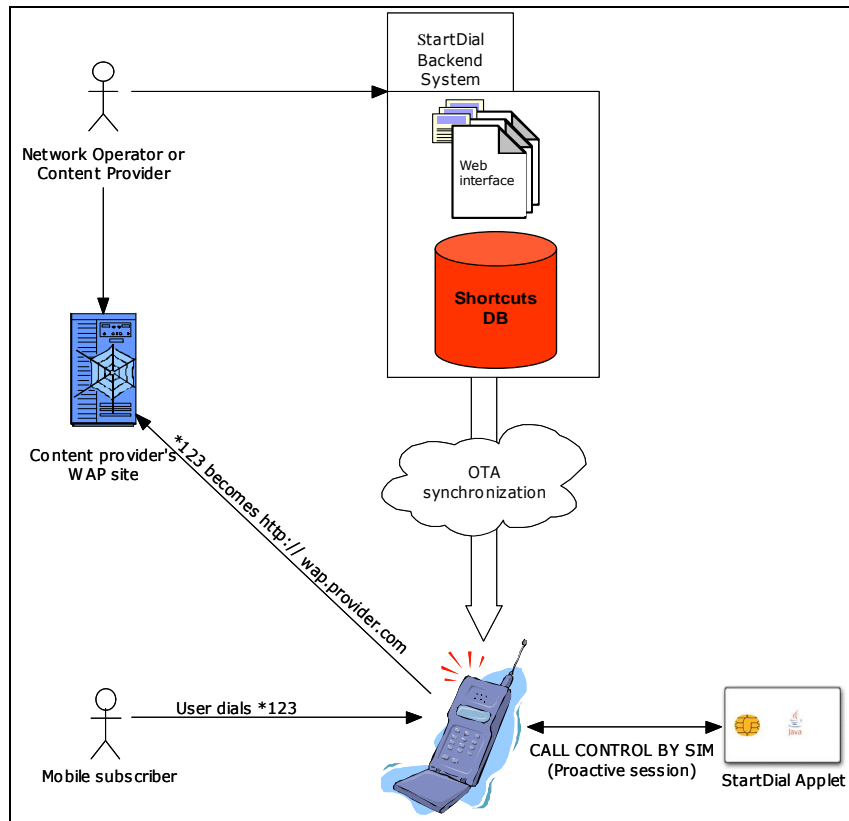
3.4. StartDial programos savybės

- Dirba bet kurioje su Java Card platforma suderinama SIM kortele;
- Atsižvelgia į telefono galimybes, kadangi ne visi supranta LAUNCH BROWSER proaktyviąją komandą;
- Pateikia automatinio papildymo (angl. auto complete) funkciją, kai yra įvedama tik pradinė trumpinio dalis;
- Palaiko vidines trumpinių duomenų bazės atnaujinimus per OTA;
- Neįtakoja įprastinių vartotojo veiksmu (skambučio, SS ar USSD simbolių rinkinio siuntimo).

3.5. StartDial architektūra

8 pav. yra pavaizduota StartDial projekto architektūra. Trumpai ją aprašysime. SIM kortelėje veikiantis Java Card apletas perima MO skambučius ar SS simbolių rinkinius prenumeruodamas „CALL CONTROL BY SIM“ įvykius ir paleidžia telefono WAP naršyklę su URL, kuris priklauso nuo rinkto (tiksliau, skambinto) numerio. URL adresai yra saugomi SIM kortelės tiesiniame-fiksuotame (angl. linear-fixed) įrašų faile ir reguliariai atnaujinami

naudojant OTA mechanizmus. Serverinė dalis valdo URL duomenų bazę ir yra atsakinga už sinchronizaciją tarp SIM kortelių OTA pagalba.



8 paveikslas. StartDial architektūra

3.6. StartDial apletas

Šio darbo metu paruošas StartDial programos kodas atitinka [GSM 03.19] reikalavimus – realizuoja *ToolkitInterface* interfeisą, taip pat pagal [JCSPEC] ir [ISS06] reikalavimus visa atmintis yra išskiriama instaliacijos, o ne vykdymo metu⁹. Trumpai aptarsime, kokias funkcijas šis apletas atlieka.

Iš karto po to, kai apletas yra instaliuojamas su LOAD (INSTALL) komanda, jis registruojasi SIM įrankių rinkinyje šioms įvykiams prenumeruoti: CALL CONTROL BY SIM ir FORMATED SMS POINT-TO-POINT ENVELOPE. Pirmasis įvykis reikalingas perimti vartotojo inicijuojamus skambučius, o antrasis naudojamas OTA sinchronizacijai atlikti.

Prieš instaliaciją SIM kortelėje turi egzistuoti tiesinis-fiksuotas EF, esantis MF direktorijoje. EF identifikacinis kodas apletu yra apibrėžtas kaip *FID_EF_SHORTCUTS*

konstanta. Šis failas yra naudojamas kaip duomenų bazė atlikti konkretaus trumpinio paieškai bei trumpinį atitinkančiam aprašymui ar URL.

Duomenys *FID_EF_SHORTCUTS* failo viduje yra saugomi naudojant paprastą TLV struktūrą. Buvo apibrėžtos trys žymės: *ST_TAG_SHORTCUT*, *ST_TAG_URL* ir *ST_TAG_NAME*. Norint pasinaudoti [GSM 11.11] apibrėžta SEEK komanda, reikalinga, kad pirmasis TLV sąrašo elementas būtų trumpinio TLV.

Kai apletas yra sužadinamas „CALL CONTROL BY SIM“ įvykio, visų pirma yra patikrinama, ar numeris, kuriuo skambinama, turi prefixą, lygų *ST_PREFIX* (apleto konstanta). Jeigu ne, tai yra indikacija nutraukti tolimesnį apleto vykdymą ir vartotojui leidžiama toliau tęsti skambutį.

Toliau yra patikrinama, ar ME palaiko skambučio kontroliavimo įvykį bei gali įvykdyti LAUNCH BROWSER proaktyvią komandą. Jeigu testas neigiamas, darbas sustabdomas.

Kitas žingsnis yra atlikti numerio, kuriuo „skambinama“ paiešką *FID_EF_SHORTCUTS* faile. Jeigu paieška gražina tik vieną rezultatą, t.y. randamas įrašas, turintis tokį patį, kaip ir įvestasis, trumpinį, tuomet einamasis skambutis yra uždraudžiamas ir yra įvykdoma LAUNCH BROWSER komanda su URL, priklausančiu trumpiniui. Kitu atveju yra atliekama automatinio papildymo procedūra, kurios paskirtis yra rasti visus trumpinius, prasidedančius „skambinamu“ numeriu. Jeigu bent vienas toks trumpinys yra randamas, su rastų trumpinių pavadinimų sąrašu (*ST_TAG_NAME*) formuojama ir įvykdoma SELECT ITEM proaktyvi komanda. Jeigu ME palaiko pagalbos užklausimus esant ant meniu punktų, papildomai prie trumpinio pavadinimo yra parodomas pagalbos tekstas su URL, į kurį veda trumpinys. Jeigu vartotojas pasirenka punktą iš sąrašo, tuomet įvykdoma LAUNCH BROWSER komanda su parametrais, kaip aprašyta aukščiau.

Tuo atveju, jeigu apletas yra sužadinamas įvykio „FORMATED SMS POINT-TO-POINT ENVELOPE“, startuojama OTA sinchronizacija. Tikimasi gauti [GSM 03.48] ENVELOPE komandos su vienos ar kelių sujungtų trumpųjų žinučių duomenimis, kurie būtų suformatuoti kaip BER-TLV duomenų struktūra. Apibrėžiame tris BER-TLV komandines žymes: *ST_CMD_NEW*, *ST_CMD_UPD* ir *ST_CMD_DEL*. Saugūs duomenys gali turėti vieną arba kelias šias žymes, kurios atitiks naujo įrašo įterpimo, esančio atnaujinimo arba įrašo pašalinimo komandas.

3.7. StartDial serverinė dalis

⁹ Tik naujausioje Java Card versijoje yra „šiukšlių surinkėjas“, todėl draudžiama dinamiškai kurti objektus, tame tarpe ir masyvus).

StartDial serverinė dalis sudaryta iš reliacinės duomenų bazės, žiniatinkliu paremtos (angl. web-based) administravimo sąsajos bei OTA mechanizmų. Jos architektūra pavaizduota 9 pav.

3.7.1. Duomenų bazės schema

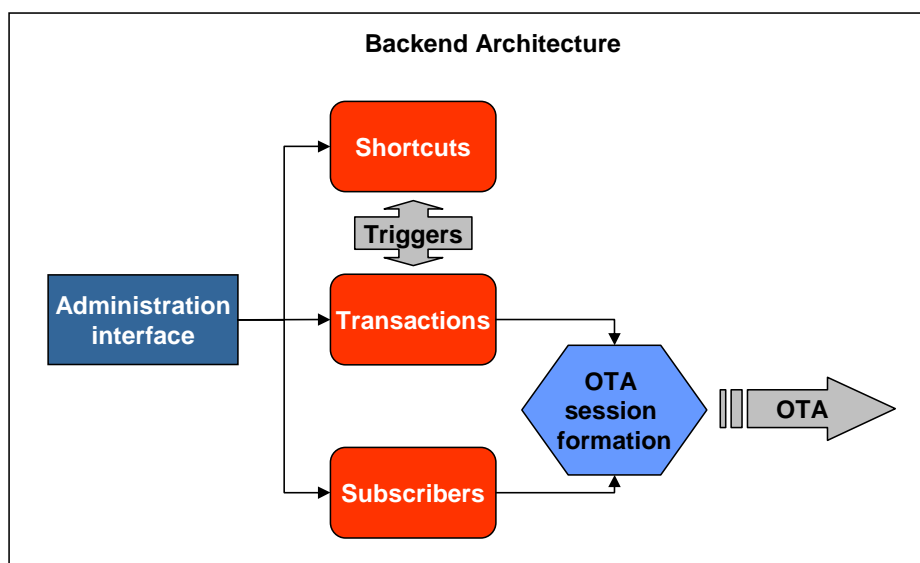
StartDial duomenų bazė saugo informaciją apie trupinius, laukiančias įvykdymo OTA transakcijas ir paslaugos naudotojus. Suprojektuota schema apima tik bazines StartDial projekto funkcijas, tačiau gali būti lengvai plečiama serverinės papildomam funkcionalumui realizuoti arba integracijai su išorinėmis sistemomis.

Duomenų bazės schemą sudaro trys lentelės: *shortcuts* (trumpiniams), *ota_transactions* (OTA transakcijoms) ir *subscribers* (paslaugos naudotojams). Trumpinių lentelę sudaro stulpeliai, aprašantys kiekvieno trumpinio savybę: *id* (identifikatorius – pirminis raktas), *shortcut* (mobilaus įrenginio atpažįstamas trumpinys, pvz. 123), *name* (trumpinio pavadinimas), *description* (trumpinio aprašas) ir *value* (trumpinį atitinkantis paslaugos URL).

Visi *shortcuts* lentelės pakeitimai trigerių pagalba bus patalpinti į *ota_transactions* lentelę, kurioje yra saugomos OTA transakcijos, kurios turės būti atliktos per artimiausią periodinę OTA sinchronizaciją, kurios metu sinchronizuojama esama trumpinių informaciją su ta, kuri yra paslaugos naudotojų SIM kortelėse.

OTA sinchronizacijų periodiškumas yra fiksuotas ir nepriklausomas nuo pavienių duomenų bazės pasikeitimų. Pavyzdžiui, gali būti pakeistas kurio nors vieno trumpinio URL arba įvestas naujas trumpinys. Toks pakeitimas neiššauks OTA transakcijos automatiškai, tačiau *ota_transactions* lentelėje bus fiksuojama nauja transakcija. *shortcut* lentelėje įvykdyta trynimo operacija *delete* sukurs laukiančią (angl. pending) *delete* tipo transakciją, įrašymo (*insert*) ir šalinimo (*delete*) operacijos irgi atitinkamai kurs transakcijas. Pagrindinis OTA sinchronizacijų sistemos tikslas yra išvengti bereikalingų transakcijų (pavyzdžiui, du atnaujinimus tam pačiam trumpiniu arba naujo trumpinio sukūrimas ir iš paskos sekantis jo pašalinimas vienos OTA sesijos metu). *ota_transactions* lentelėje saugoma informacija yra naudojama paslaugos naudotojų, kuriems reikalinga atnaujinti SIM kortelės trumpinių duomenų bazę, sąrašas.

Lentelėje *subscribers* yra saugoma informacija apie paslaugos naudotojus bei kiekvieno jų lokalią duomenų bazę, papildytą paskutinių OTA atnaujinimų metų. Šioje lentelėje taip pat saugomas kiekvieno paslaugos naudotojo paskutinio OTA atnaujinimo tiksli data ir laikas. Ši informacija, kartu su *ota_transaction* lentelės duomenimis yra naudojama paslaugos naudotojų sąrašo, kuriems reikalingi OTA atnaujinimai, formavimui.



9 paveikslas. Startdial serverinės dalies architektūra

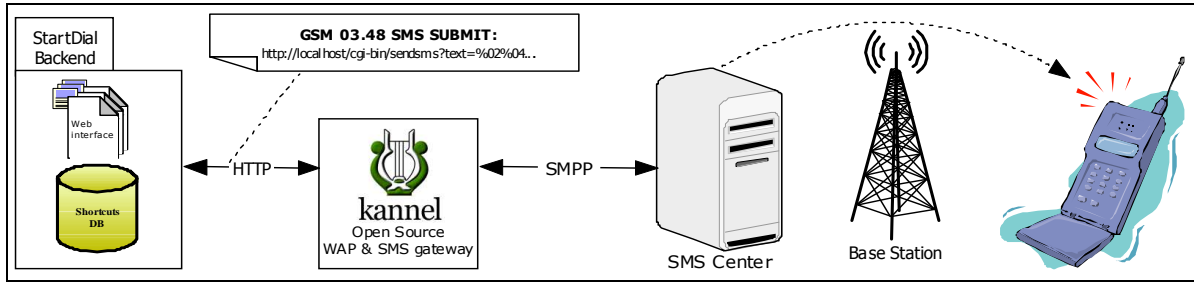
Kaip jau minėta, šios, palyginti paprasto schemos pakanka atlikti bazinės sistemos testavimo procedūras. Pilna duomenų bazės schema galėtų būti išplėsta papildomomis funkcijomis, pavyzdžiui, automatizuotas OTA transakcijų būsenos, paremtos žinučių gavimo ataskaitomis (angl. delivery reports) fiksavimas, paslaugos partnerių duomenų baze, kurią sudarytų informacija apie partnerių valdomas paslaugas ir pan.

Atliekant šį darbą buvo sukurtas žiniatinkliu paremtas bazinis administravimo įrankis duomenų bazės schemos valdymui. Šio įrankio pakako darbui su minėtų duomenų bazių lentelių duomenimis.

3.7.2. OTA mechanizmai

Over-the-Air transakcijos yra naudojamos trumpinių informacijos perkėlimui paslaugos naudotojams. Kiekvienas mobilusis įrenginys turi SIM paremtą trumpinių failą, kuris atnaujinamas po pasikeitimų serverinės dalies centrinėje duomenų bazėje. StartDial OTA mechanizmų diagrama yra pavaizduota 10 pav.

OTA transakcijų sesijos yra atliekamos nustatytais laiko intervalais ir vykdo informacines transakcijas kiekvienam paslaugos naudotojui. Trumpinių informacijos perdavimui buvo sukurtas TLV struktūra paremtas protokolas, pavaizduotas 6 lentelėje. Šio protokolo žinutę sudaro operacinės žymės, kurios nusako įrašymo (*insert*), atnaujinimo (*update*) ar šalinimo (*delete*) operacijas, ilgio informacija bei trumpinys, jo pavadinimas ir reikšmė (URL).



10 paveikslas. OTA mechanizmų diagrama

OTA žinučių perdavimui reikalingas įrankis, galintis interneto protokolu (IP) SMS centrui perduoti trumpąsias SMS žinutes, suformatuotas pagal [GSM 03.48] reikalavimus. Vienas iš būdų yra naudoti atvirojo kodo WAP ir SMS žinučių šliuzą Kannel (<http://www.kannel.org/>), kuris leidžia ne tik palyginti nesunkiai įvairiais SMS centrų protokolais (pavyzdžiui, SMPP) prisijungti prie SMS centro ir siųsti bei gauti žinutes, tačiau kartu automatizuoja ilgų žinučių (viršijančių 140 baitų) skaidymą į atskirus segmentus.

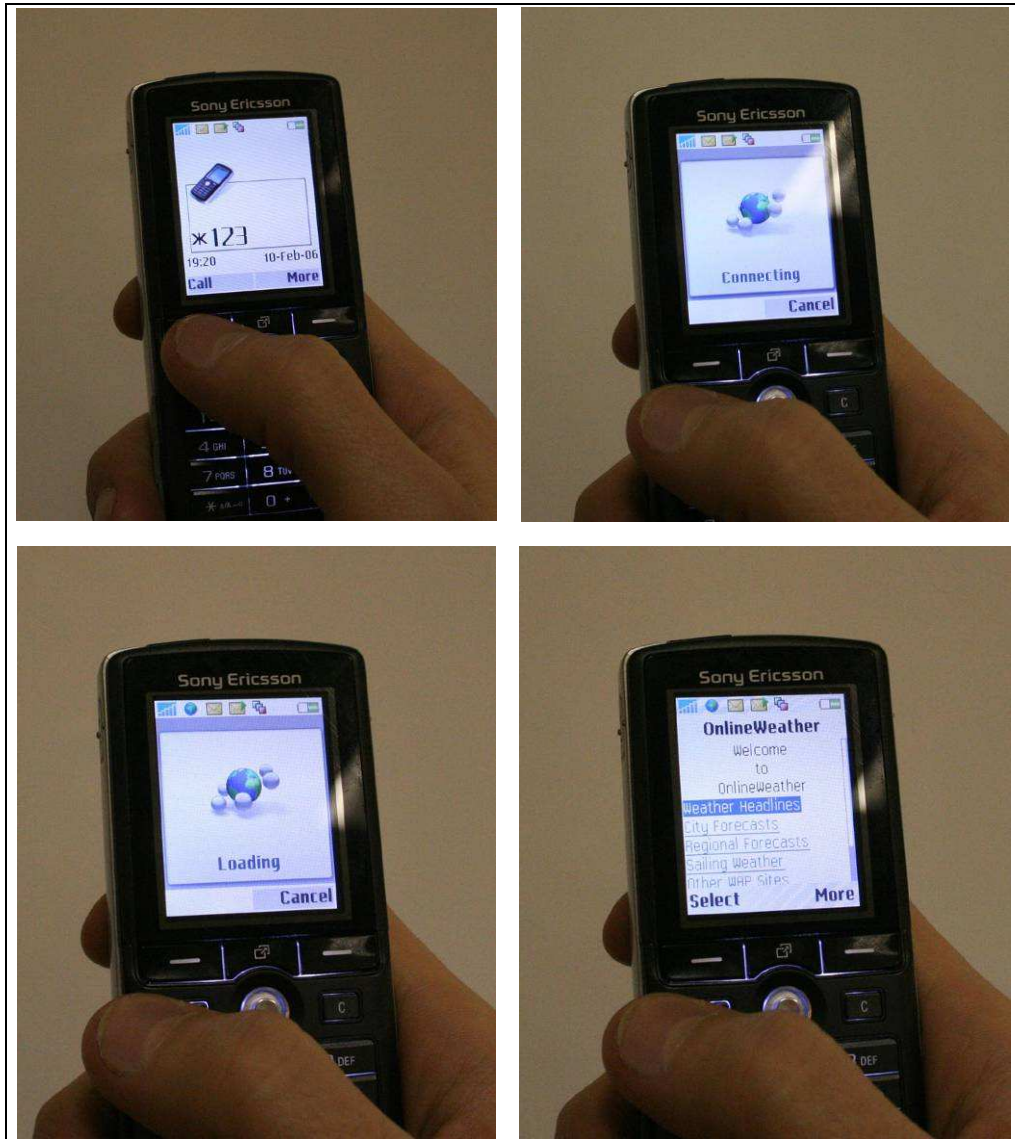
Tag	Length	Value		
		Tag	Length	Value
<i>ST_CMD_NEW</i>	Komandos ilgis	<i>ST_TAG_SHORTCUT</i>	Komandos ilgis	Trumpinys (pvz. 123)
<i>ST_CMD_UPD</i>		<i>ST_TAG_URL</i>		Trumpinį atitinkantis URL
<i>ST_CMD_DEL</i>		<i>ST_TAG_NAME</i>		Trumpinio pavadinimas

6 lentelė. BER-TLV protokolo žinutės

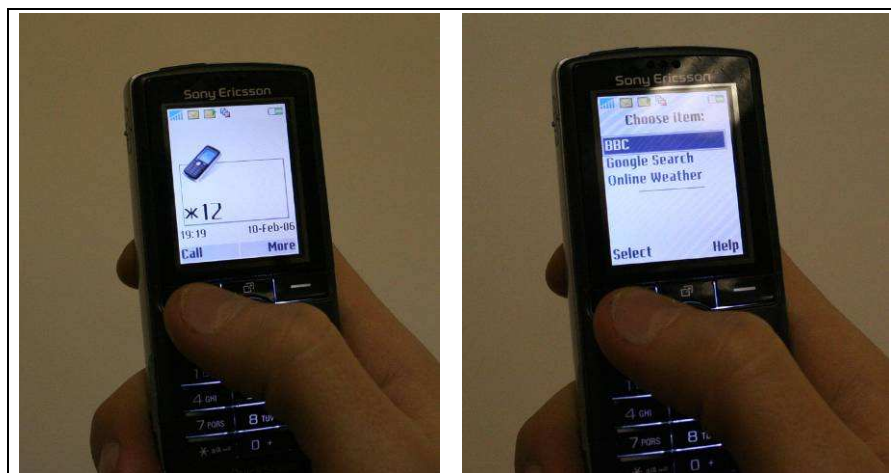
3.8. Testavimas

Veikiantis StartDial prototipas buvo sėkmingai ištestuotas su keliais populiariausių gamintojų mobiliaisiais telefonais: Nokia, Sony-Ericsson, Siemens ir Motorola. Nepaisant to, kad kai kurie testuoti telefonai specifines funkcijas atliko kiek skirtingai, tačiau tiek bazinės, tiek papildomos (pvz. automatinio papildymo) funkcijos veikė taip, kaip ir tikėtasi ant daugelio naujesnių telefonų modelių, palaikančių raidės klasę „c“, į kurią įeina ir „LAUNCH BROWSER“ proaktyvi komanda [GC02].

Testavimo duomenims sukurti buvo naudotas šio darbo pirmajame priede pateiktas skriptas Python skriptavimo kalba, kuris sugeneruoja BER-TLV žinutę su dviejų naujų trumpinių ir juos atitinkančių URL įrašymu (dvi *ST_CMD_NEW* komandos). Norint šią žinutę nusiųsti ME, papildomai reikėtų pritaikyti [GSM 03.48] kodavimą pagal SIM kortelės saugumo reikalavimus.



11 paveikslas. StartDial bazinis funkcionalumas



12 paveikslas. StartDial automatinio papildymo funkcionalumas

11 pav. ir 12 pav. yra pavaizduoti StartDial programos testai su mobiliuoju telefonu Sony Ericsson T610.

11 pav. yra demonstruojamas bazinis StartDial funkcionalumas – visų pirma telefono klaviatūra yra surenkamas trumpinys (*123), tuomet paspaudžiamas skambinimo mygtukas. Vietoj skambučio užmezgimo yra vykdoma LAUNCH BROWSER proaktyvi komanda, kuriai kaip parametras yra perduodamas trumpinį *123 atitinkantis URL <http://wap.onlineweather.com>¹⁰. Jeigu telefono WAP naršyklės nustatymai yra korektiški, telefonas užmezga ryšį su numatyta GPRS sąsaja (angl. APN) ir WAP naršyklėje parodo orų svetainę.

12 pav. yra pavaizduotas papildomas StartDial funkcionalumas – automatinis trumpinių papildymas. Telefono naudotojui įvedus tik dalį trumpinio (*12) ir paspaudus skambinimo mygtuką, skambutis taip pat yra nutraukiamas ir telefone yra formuojamas visų trumpinių, kurie prasideda „skambinamuoju“ prefiksu, sąrašas¹¹. Jeigu ME palaiko pagalbos funkciją sąrašo elementui, tuomet, priklausomai nuo telefono modelio, arba palaukus kelias sekundes, arba paspaudus pagalbos mygtuką galima pamatyti visų trumpinių, prasidedančių su įvestu prefiksu, pavadinimus. Paspaudus ant pasirinkto trumpinio, atliekami tie patys veiksmai, kaip ir įvedus pilną trumpinį – startuojama WAP naršyklė su trumpinį atitinkančiu URL.

3.9. Galimos papildomos funkcijos bei savybės

Savybė	Aprašymas
Perėjimas prie serverine dalimi paremto arba mišraus sprendimo.	Jeigu reikalingas paslaugos naudotojo veiksmų fiksavimas arba papildomos informacijos suteikimas paslaugos partneriams, gali būti reikalinga dalį veiksmų iš apleto perkelti į serverinę dalį.
Išplėsti dabartinį naršyklės paleidimo veiksmą į skambučio užmezgimą ar trumposios žinutės išsiuntimą.	Realus trumpinio „skambinimo“ veiksmas gali neapsiriboti vien tik naršyklės paleidimu. Tam tikriems trumpiniams, priklausomai nuo jų specifikos, įmanoma įgyvendinti tiek „Send SMS“, tiek „SET UP CALL“ komandų įvykdymą.

¹⁰ Žr. testinius duomenis pirmajame priede.

¹¹ Sąrašas formuojamas SELECT ITEM proaktyvia komanda.

<p>Trumpąja žinute informuoti ryšio paslaugų tiekėją apie tris nesėkmingus bandymus paleisti telefono naršyklę. Papildomai galima informuoti apie naudojamo telefono aparato savybes.</p>	<p>Keli nesėkmingi telefono naršyklės paleidimo bandymai gali būti nuoroda ryšio paslaugų tiekėjui, kad paslaugos vartotojui turi būti nusiųsti aktyvūs OMA/OTA tinklo nustatymai.</p>
---	--

4. Mobilusis elektroninis parašas

Elektroninis parašas gali būti tikrinamas ne tik namų aplinkoje, įstaigoje ar viešosiose vietose, bet ir mobiliojoje aplinkoje [UND03]. Elektroninio Parašo Proveržio Programos [E3P] wPKI Specifikacijoje numatyta, kad „wPKI yra paremta SIM Toolkit-standartu“. Vadinasi, šiai sistemai galiotų panašūs principai, kaip ir aptartame StartDial projekte. Pastarojoje specifikacijoje nėra kalbama apie konkrečią SIM kortelių, kuriose būtų diegiamas mobilusis elektroninis parašas, platformą, tačiau pasirinkus Java Card technologiją, atsiranda galimybė naudoti vieningą sąsają (API) raktų valdymui bei duomenų pasirašymui. [JCSPEC] apibrėžtas *javacard.security* paketas numato visą aibę klasių, skirtų darbui su viešuoju ir privačiuoju raktais, sertifikatais, bei metodus duomenų pasirašymui, naudojant DSA ir RSA algoritmus. Šiame darbe aprašytus OTA mechanizmus būtų galima sėkmingai panaudoti elektroninio parašo pasirašymui reikalingų transakcijų inicijavimui, kai telefono naudotojui būtų suformuojamas transakciją reikalaujantis patvirtinti dialogas.

Šiame skyriuje išnagrinėsime technologines priemones, reikalingas wPKI infrastruktūrai realizuoti. Visų pirma pastebėsime, kad nei antrosios (2G, 2.5G), nei trečiosios (3G) kartos mobiliojo ryšio tinkluose viešojo rakto infrastruktūra PKI tradicinėms paslaugoms teikti iki šiol plačiai nebuvo naudojama. Tai lemia trys pagrindinės priežastys [DGSW02]:

- slaptas raktas (angl. secret key), kuris turi būti iš anksto žinomas mobiliam įrenginiui (pvz. intelektualiai kortelei) bei paslaugos tiekėjui, gali būti sąlyginai nesudėtingai įdiegtas kaip kontrakto sudarymo dalis;
- neišsigynimas (angl. non-repudation) nėra griežtas reikalavimas prieigai prie tinklo;
- simetrinė kriptografija užtikrina kur kas didesnę našumą nei viešojo rakto kriptografija.

4.1. WTLS ir WIM

Vis dėlto reikia išskirti dvi mobiliąsias technologijas, kuriose yra naudojama PKI. Tai WAP 1.2 standarte numatyti bevielio transporto sluoksnio apsaugos protokolas WTLS bei WAP identifikacijos modulis WIM.

WTLS technologija yra naudojama saugiam ryšiui tarp mobiliojo įrenginio ir WAP šliuzo užtikrinti. Kadangi WTLS protokolas nėra suderinamas su TLS, WAP šliuzas turinį turi dekoduoti prieš persiūsdamas jį toliau turinio serveriui. Tai reiškia, kad WTLS neužtikrina vienašalio (angl. end-to-end) saugumo tarp mobiliojo įrenginio ir turinio serverio. Kitaip tariant, yra naudojama taip vadinama pasitikėjimo grandinė (angl. chain of trust), kuomet

klientas „pasitiki“ WAP šliuzu, o pastarasis savo ruožtu atlieka tarpininko vaidmenį. WAP 2.0 protokolo versija nebereikalauja WAP šliuzo elemento, kadangi telefonai tiesiogiai palaiko TCP/IP protokolą. Daugelis telefonų taip pat palaiko TLS bei SSL protokolus, o tai reiškia, kad vienašalis saugumas gali būti užtikrinamas be WAP šliuzo pagalbos, t.y. tiesiogiai tarp mobiliojo įrenginio ir turinio serverio. Kitaip tariant, WAP 2.0 iš esmės atitinką modelį, kuris yra naudojamas įprastinėse interneto naršyklėse.

WIM modulis yra naudojamas kaip priedas WTLS funkcijoms iš taikomųjų programų atlikti. Jis apibrėžia slaptų raktų bei sertifikatų, reikalingų autentifikacijai ir neišsigynimui užtikrinti, saugojimą bei panaudojimą. Siekiant užtikrinti apsaugotą laikmeną (angl. tamper resistance), WIM yra realizuojamas kaip programinė įranga mikroprocesorinėje intelektualiojoje kortelėje. WAP standarte apibrėžtoje skriptavimo kalboje WMLscript, naudojamoje WML puslapiuose, yra *signText* procedūra, kuri leidžia dirbti su elektroniniu parašu. *signText* funkcija mobiliam vartotojui leidžia elektroniniu būdu patvirtinti transakcijas taip, kad jas vėliau galėtų patikrinti turinio serveris. Tokiu būdu yra užtikrinamas vienašalė mobilus vartotojo autentifikacija, kartu išlaikant transakcijos vientisumą bei neišsigynimą [NL04].

Minėtos WTLS ir WIM technologijos yra pagrindas beveik visam viešojo rakto infrastruktūrai wWPKI. Iš esmės tai yra optimizuotas tradicinės PKI variantas, kuriam reikalingi šie komponentai: galutinė taikomoji programa (EE – End-Entity Application), registravimo organizacija (RA – Registration Authority), sertifikavimo organizacija (CA – Certification Authority) bei PKI repozitorija. WPKI apibrėžia tris transporto sluoksnio sesijos saugumo lygius: 1, 2 ir 3 WTLS klases bei *signText* f-ją – WMLscript funkcionalumą elektroniniams parašams:

- 1 klasė – WTLS kriptavimas;
- 2 klasė – kriptavimas ir šliuzo autentifikacija;
- 3 klasė – kriptavimas ir dvipusė autentifikacija.

WTLS atveju turinio serveris patvirtina savo autentiškumą WAP šliuzui siųsdamas elektroninį SSL formato sertifikatą. Tą patį atlieka ir WAP šliuzas, kuris siunčia savo sertifikatą mobiliam klientui. Tiek turinio serverio, tiek WAP šliuzo sertifikatai yra išduoti vieningos CA, kurios šakninis sertifikatas yra saugomas tiek WAP šliuze, tiek mobiliame įrenginyje. Šakninis sertifikatas mobiliame įrenginyje yra saugomas WIM modulyje kompaktiškoje formoje, dar vadinamoje WTLS sertifikatu. Saugumo sumetimais mobilus

klientas taip pat turi turėti galimybę patikrinti, ar WAP šliuzo sertifikatas nebuvo atšauktas. Nors egzistuoja nemažai techninių sprendimų tokiam patikrinimui, mobilaus ryšio atveju toks patikrinimas nėra įmanomas dėl daugelio apribojimų, todėl vienintelis sprendimas yra trumpalaikių sertifikatų naudojimas WAP šliuze. Iš mobilaus kliento pusės, galimi du autentiškumo užtikrinimo mechanizmai:

- naudojant WTLS 3 klasę tarp kliento ir šliuzo;
- naudojant WMLscript elektroninius parašus tarp mobilaus kliento ir turinio serverio.

Išvardintiems metodams yra būtina, kad privatus raktas ir skaitmeninis sertifikatas būtų saugomas WIM modulyje. Kliento autentiškumui atlikti klientui yra reikalinga turėti URL nuorodą į pilną SSL sertifikatą, kuris dažnai yra per didelis saugojimui mobiliajame telefone. Visos šalys, įtrauktos į mobiliųjų mokėjimų sistemą, turi prieigą prie pilnos versijos SSL sertifikatų.

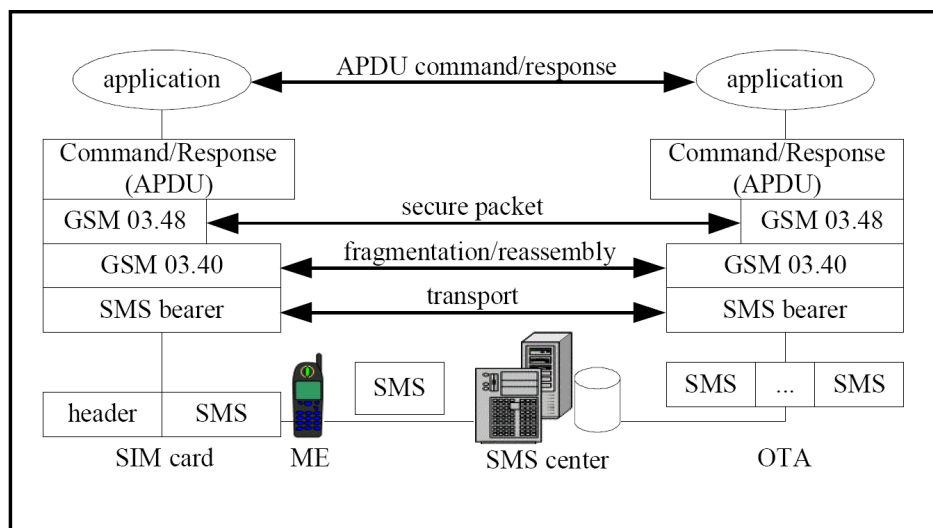
Galima išskirti keturis pagrindinius WTLS technologijos trūkumus:

- WAP šliuzas sukuria galimą saugumo spragą, kadangi turi prieigą prie atkoduotų vartotojo duomenų;
- Vartotojas gali autentifikuoti tik WAP šliuzą, tačiau ne turinio serverį;
- Nėra privataus-viešojo rakto porų generavimo vartotojo įrenginyje palaikymo;
- Nėra lokalių duomenų kodavimui vartotojo įrenginyje palaikymui.

Šios ir kitos priežastys lėmė tai, jog WTLS technologija niekada nebuvo plačiai paplitusi tarp mobiliųjų įrenginių bei WAP šliuzų. Kaip jau minėjome, WAP 2.0 protokolą palaikantys mobilieji įrenginiai (tokių dabar dauguma) su išoriniais žiniatinklio serveriais bendrauja tiesiogiai TCP/IP protokolu. Kitaip tariant, WTLS tampa apskritai nebereikalingas, kadangi didžioji dalis WAP 2.0 įrenginių taip pat gali dirbti TLS bei SSL protokolais, tokiu būdu užtikrinant saugų ryšį su konkrečiu žiniatinklio serveriu be tarpininkų (WTLS atveju – WAP šliuzą). Kitą WPKI elementą – WIM modulį – bandyta pritaikyti kai kuriuose mobilaus elektroninio parašo sprendimuose, tačiau tai netapo de-facto standartu.

4.2. STK saugumo mechanizmai

Kaip jau minėta 1-ajame šio darbo skyriuje, saugiam duomenų apsikeitimui tarp SIM taikomųjų programų ir išorinių sistemų užtikrinti yra naudojami [GSM 03.48] standarte numatyti saugumo mechanizmai. Apžvelgsime juos detalčiau.



13 paveikslas. Duomenų apsikeitimas tarp SIM ir OTA [BU04]

Tiek telefono, tiek bet koks kitas įrenginys neturi tiesioginės prieigos prie SIM kortelės atminties. Bet koks komunikavimas (įskaitant nuotolinį failų bei taikomųjų programų valdymą, apie kurios jau kalbėjome šiame darbe) vyksta APDU pagalba, tame tarpe ir [GSM 03.48] standarte numatytas nuotolinis bendravimas OTA tiek su SIM kortele, tiek su joje įdiegtomis STK taikomosiomis programomis. Pastaruoju atveju APDU komandos yra inkapsuliuojamos į OTA žinutes, kurios teoriškai yra nepriklausomos nuo protokolo, tačiau daugeliu atveju transportavimui pasitelkiamos trumposios SMS žinutės. Naujesni SIM standartai OTA komunikavimui numato nuo nešmenos nepriklausomą protokolą BIP, tačiau tik nedaugelis rinkoje esančių mobiliųjų įrenginių jį palaiko. BIP protokolas leidžia OTA komandas vykdyti naudojant Bluetooth, GPRS ir kitas nešmenas.

OTA mechanizmams operatoriaus infrastruktūroje yra reikalingas OTA šliuzas, kuris APDU komandas sugebėtų transliuoti į SMS žinutes bei perduotų į SMS centrą, o pastarasis – į SIM kortelę. Kiekviena OTA žinutė, kuri yra siunčiama į ar iš SIM kortelės, yra koduojama simetriniais raktais, kurie yra priskiriami kiekvienai SIM kortelei. Raktai yra saugomi elementariuosiuose failuose (EF), prie kurių prieiga yra griežtai apribota, siekiant išvengti neautorizuoto jų panaudojimo. Kaip tik pranešimų konfidencialumą ir vientisumą, šalių autentiškumą bei atkartojimo detektavimo mechanizmus numato [GSM 03.48] standartas.

Žinutės integralumas užtikrina, kad žinutė pakeliui nebuvo iškraipyta ar kaip nors kitaip pakeista. Konfidencialumo funkcija apsaugo nuo taip vadinamosios trečiosios šalies, galinčios peržiūrėti siunčiamų saugių paketų turinį. Atkartojimo detektavimo mechanizmai priimančiajai šaliai leidžia išvengti pakartotinio paketų gavimo, taip apsisaugant nuo pakartojimų atakų (angl. replay attacks). Autentiškumo mechanizmas yra naudojamas OTA komunikavimą dalyvaujančią šalį apsaugoti nuo neautorizuoto panaudojimo. Šis mechanizmas užtikrina, kad tik autorizuotos šalys gali vykdyti veiksmus su SIM kortelės failais, taip pat neautorizuotoms šalims užkerta kelią prieigai prie SIM kortelės duomenų. Verta paminėti, kad SMS nešmena yra vienakryptis transporto mechanizmas, todėl abipusė autentifikacija antrosios kartos GSM tinkle nėra numatyta [BU04].

Svarbu paminėti, kad vienoje SMS žinutėje realių duomenų galima perduoti 140 baitų. Norint nusiųsti ilgesnį pranešimą, reikalingas žinučių jungimas, kuris atliekamas prie kiekvienos žinutės pridendant vartotojo duomenų antraštę UDH (angl. User Data Header), kuri papildomai užima dar 6 baitus. Priklausomai nuo to, kokie [GSM 03.48] saugumo mechanizmai naudojami (pranešimų konfidencialumo ir vientisumo, šalių autentiškumo bei atkartojimo detektavimo užtikrinimą galima taikyti kartu, tačiau nebūtinai, pvz., galima atsisakyti konfidencialumo nekoduojuojant pačių duomenų), naudingasis žinutės tūris taip pat ženkliai sumažėja, todėl vienoje žinutėje realių duomenų galima perduoti ne daugiau negu 113 baitų. Vienos SMS žinutės pristatymas mobiliojo ryšio įrenginiui vidutiniškai užtrunka 3–4 sekundes, todėl norint OTA pagalba perduoti didesnius duomenų kiekius (pvz. dokumentą, kurį norimą pasirašyti elektroniniu parašu), tai gali labai ilgai. Taip pat reikia turėti omenyje, jog ilgo¹² pranešimo pristatymo metu telefono įrenginys gali laikinai būti nepasiekiamas, o tai reiškia, kad OTA šliuzas turi gebėti sekti, kurios iš pranešimo dalių buvo sėkmingai pristatytos ir pakartotinai bandyti pristatyti tik dar nepristatytas dalis. Tas pats galioja ir SIM kortelei, kuriai norint pratęsti nutrūkusią ilgojo pranešimo priėmimo seriją reikalinga pranešimo dalis kaupti pastovios atminties (EEPROM) buferyje. Kadangi SIM kortelių atmintis yra ribota, šis funkcionalumas ne visuomet yra realizuotas.

4.3. Java Card saugumo sąsajos

Šiame poskyryje trumpai apžvelgsime Java Card 2.1 specifikacijoje numatytas saugumo sąsajas (API), tiksliau – joje apibrėžtą *javacard.security* paketą, kuris apibrėžia darbą su simetriniais ir asimetriniais raktais bei priemonės asimetrinių raktų poros sukūrimui, žinutės santraukai skaičiuoti, atsitiktiniams duomenims generuoti ir duomenims pasirašyti.

¹² T.y. sudaryto iš kelių SMS, naudojant jungimo mechanizmus

4.3.1. **javacard.security** klasės

javacard.security paketas apibrėžia šias **abstrakčias** klases: *KeyBuilder*, *Signature*, *MessageDigest*, *RandomData* ir *CryptoException*. Trumpai aptarsime kiekvieną iš jų.

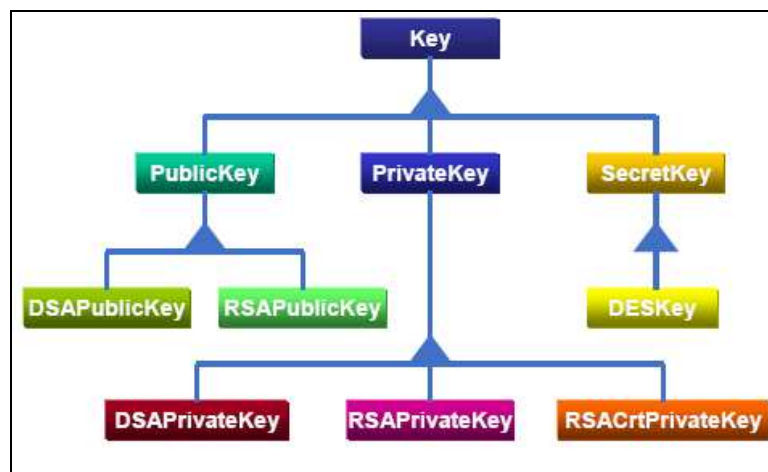
- *KeyBuilder* – raktų objektų „gamykla“, skirta kurti kriptografinius raktus. Naudojama parašo ir šifravimo algoritmuose. Gražinamas objektas turi būti paverstas (angl. cast) į atitinkamą rakto tipo interfeisą. Tik šios „gamyklos“ sukurti raktai gali būti naudojami *Signature* ir *Cipher* (pastaroji apibrėžtas *javacardx.crypto* pakete) klasių egzempliorių inicializavimui.
- *MessageDigest* – bazinė santraukų algoritmų klasė. Apibrėžti MD5, SHA ir MD-160 algoritmai.
- *RandomData* – atsitiktinių skaičių generavimas.
- *Signature* – parašo skaičiavimo klasė. Apibrėžti keli skirtingi (pvz., DES-CBC, DES-ECB) algoritmai bei RSA ir DES papildymo (angl. padding) schemas, kurios reikalingos dėl viešojo rakto algoritmuose žinutės santrauką transformuoti į kodavimo bloko dydį (angl. encryption block size).
- *CryptoException* – išskirtinių situacijų (angl. exceptions) klasė.

4.3.2. **javacard.security** interfeisai

javacard.security paketas taip pat apibrėžia šiuos interfeisus: *Key*, *SecretKey*, *DESKey*, *PublicKey*, *RSAPublicKey*, *DSAPublicKey*, *PrivateKey*, *DSAPrivateKey*, *RSAPrivateKey* ir *RSAPrivateCrtKey*. Visi interfeisai yra *Key* tipo, t.y. *Key* yra tėvinis visų kitų interfeisų interfeisas. Paveldėjimo hierarchija yra pavaizduota 14 pav.

Key interfeise apibrėžti baziniai primityvai rakto dydžiui ir tipui gauti, o *PublicKey*, *PrivateKey* ir *SecretKey* jokių metodų nenusako, tačiau yra baziniai interfeisai atitinkamai išvestiniams viešojo, privataus ir simetrinio raktų interfeisams. *DESKey* yra skirtas saugoti 8, 16 ir 24 baitų raktą atlikti dviejų ar trijų raktų reikalaujančiai trigubai (angl. triple) operacijai atlikti. 14 pav. nepavaizduotas *DSAKey* yra bazinis interfeisas DSA algoritmu paremtomis viešojo ir privataus rakto realizacijoms. Likusi interfeisų šeima yra skirta duomenų pasirašymui su RSA tipo privačiu ir viešuoju raktais¹³.

¹³ *RSAPrivateKey* ir *RSAPublicKey* bei *RSAPrivateCrtKey*, pastaroji naudoja kinų liekanos teoremos – Chinese Remainder Theorem – formą.



14 paveikslas. javacard.security raktų interfeisų paveldėjimo hierarchija

4.3.3. Java Card specifikacijos versijos ir realizacija

Verta pastebėti, kad naujoje Java Card specifikacijos versijoje 2.2.2 javacard.security paketas yra papildomas (lyginant su 2.1 versija) šiomis pagrindinėmis savybėmis [JC222]:

- AES tipo simetrinių raktų palaikymas (įvedamas naujas *AESKey* interfeisas).
- Elipsinės kreivės privataus ir viešo rakto algoritmo EC palaikymas (įvedami nauji *ECKey*, *ECPrivateKey* ir *ECPublicKey* interfeisai).
- Papildomai palaikomi šie santraukos algoritmai: SHA-256, SHA-384 ir SHA-512.
- Papildomai palaikomi šie parašo algoritmai: ISO9796-2, HMAC ir Korean SEED NOPAD.
- Įvedamas *HMACKey* interfeisas, skirtas HMAC algoritmo raktų inkapsuliavimui.
- Įvedama *KeyPair* abstrakti klasė, skirta saugoti privataus (*PrivateKey*) ir viešojo (*PublicKey*) raktų porą.

Šiuo atveju gana svarbi naujovė yra būtent elipsinės kreivės kriptografijos ECC¹⁴ bei elipsinės kreivės skaitmeninio parašo algoritmo ESDSA¹⁵ įvedimas. RSA (Rivest-Shamir-Adleman) viešojo rakto algoritmo vienas pagrindinių trūkumų yra palyginti ilgas duomenų kodavimo laikas, ypač jeigu dirbama montuojamuose (angl. embedded) įrenginiuose, tokiuose, kaip SIM kortelė.

¹⁴ Elliptic Curve Cryptography

¹⁵ Elliptic Curve Digital Signature Algorithm

163 bitų ECC garantuoja nemažesnę saugumą nei 1024 bitų RSA, kuris šiandien vis dar labai plačiai naudojamas. Tyrimas parodė, kad 163 bitų ECC vykdymo laikas buvo maždaug penkis kartus trumpesnis lyginant su 1024 bitų RSA, o bendras ECC skaičiavimams atlikti reikalingas resursų kiekis yra mažesnis nei RSA. Todėl ECC šiuo požiūriu yra tinkamesnis saugiuose ribotų skaičiavimo ir atminties resursų įrenginiuose – intelektualiosiose kortelėse ir pan. [HKJCS02]

Kaip jau minėta, Sun Microsystems pateikiamoje Java Card specifikacijoje yra aprašyti tik interfeisai ir abstrakčios klasės. Tai reiškia, kad konkreti realizacija paliekama intelektualiosios kortelės gamintojui. Paprastai PKI skaičiavimus atliekančios kortelės yra komplektuojamos kartu su mašininio ko-procesoriumi, tokiu būdu užtikrinant spartesnę laikui imlių operacijų (dažniausiai RSA ir/ar ECC) darbą.

Svarbu pastebėti, kad nei Java Card specifikacija, nei SIM kortelių standartai aiškiai nenumato fizinės sertifikato, viešojo bei privataus raktų fizinės būvimo vietos. Kitaip tariant, taikomajai programai – Java Card apletui – norint atlikti konkrečius su elektroniniu parašu susijusius veiksmus, reikalingas būdas gauti nuorodą į aktyvų privataus rakto (arba kitus PKI elementus) egzempliorių (raktai paprastai turėtų būti sugeneruojami prieš išduodant SIM kortelę, t.y. personalizacijos fazėje). Šiame darbe jau minėtas [WIM] standartas apibrėžia primityvius darbui su simetriniais bei asimetriniais raktais, duomenų kodavimu ir skaitmeniniu parašu. Standarte yra numatytos APDU komandos bei elementariųjų failų struktūra raktams saugoti [WIM], tačiau standartas yra daugiau orientuotas į WIM taikymą su WTLS technologija bei į tai, kad veiksmus inicijuoja mobilusis įrenginys (ME), o ne SIM kortelė ar joje veikianti taikomoji programa. Taigi Java Card SIM kortelėse privataus ir viešojo raktų pora saugoma priklausomai nuo konkrečios realizacijos, pavyzdžiui, kaip atskiras apleto egzempliorius, pasiekiamas per *Shareable* interfeisą.

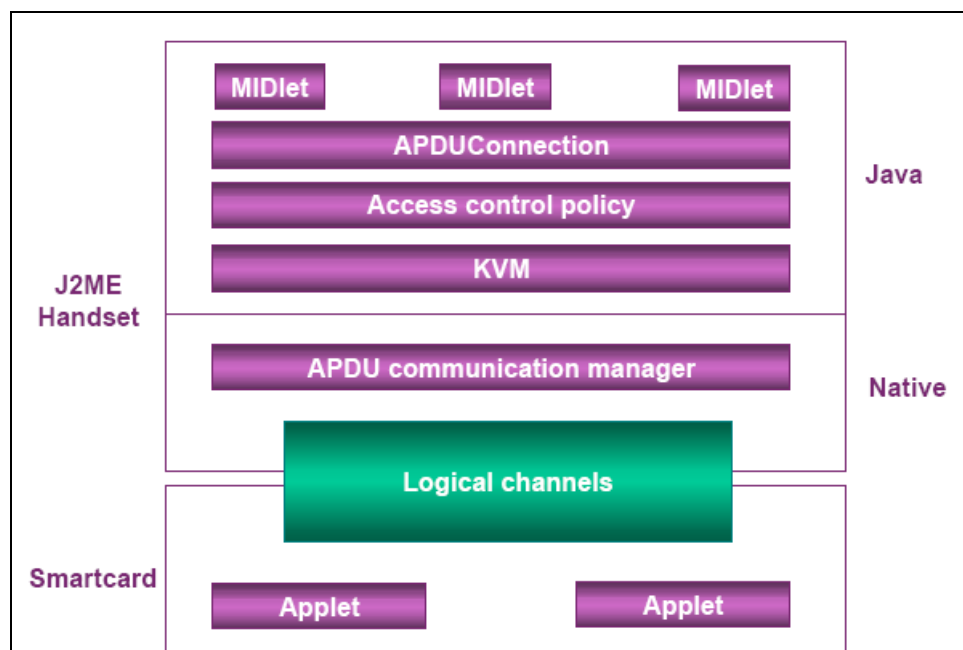
4.4. SATSA / JSR 177

Mobiliosios Java J2ME redakcijos MIDP profilio 2.0 versija numato neprivalomą SATSA paketų rinkinį, skirtą išplėsti J2ME saugumo savybes bei įgalinti J2ME taikomąsias programas (midletus) bendrauti su intelektualiąja kortele. Paketą apibrėžia Java specifikacijos užklausa JSR¹⁶ 177, prie kurios sudarymo prisidėjo stambiausi intelektualiuųjų kortelių gamintojai bei mobiliojo ryšio operatoriai.

[JSR177] pagalba atsiranda galimybė realizuoti dideliu saugumu pasižyminčias taikomąsias programas, kur J2ME yra atsakinga už vartotojo sąsają bei bendravimą su

¹⁶ Java Specification Request

išoriniu pasauliu (pavyzdžiui, bankinėmis sistemomis), tuo pačiu siunčiamus duomenis koduoti raktu, saugomu SIM kortelėje. Tai yra daroma pasinaudojant šiame darbe jau minėta Java Card RMI technologija – *Shareable* interfeisu, kurį turėtų realizuoti SIM kortelėje veikiantis apletas arba APDU komandomis. Bendra J2ME komunikavimo su intelektualiąja kortele schema pavaizduota 15 pav.



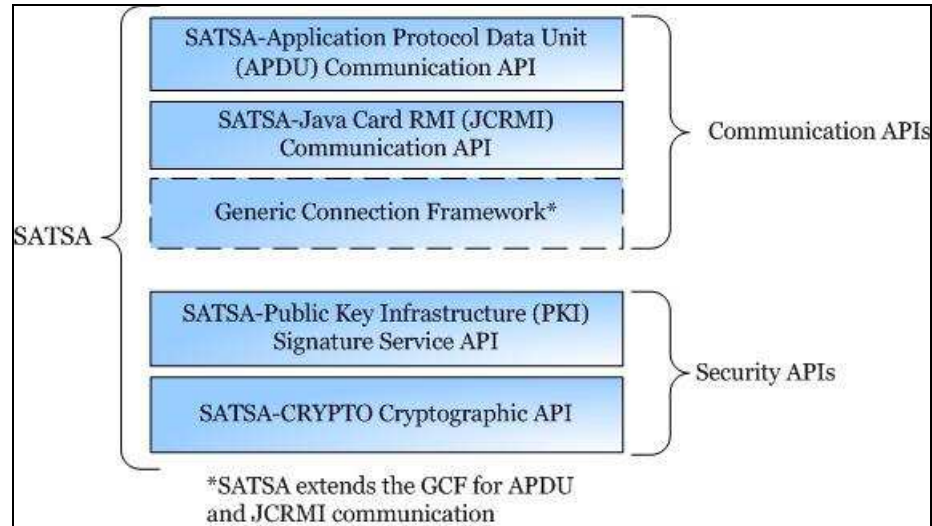
15 paveikslas. SATSA-APDU komunikavimo modelis [NAC06]

SATSA neprivalomų paketų rinkinį sudaro šie keturi paketai [ORT05], kurie schematiškai pavaizduoti 16 pav.:

- SATSA-APDU komunikavimo sąsaja – APDU protokolo palaikymas. Svarbu paminėti, kad vienintelė leidžiama komanda yra *ENVELOPE* APDU, o proaktyvios sesijos ir komandos nėra palaikomos.
- SATSA-JCRMI komunikavimo sąsaja – Java Card 2.2 specifikacijoje apibrėžto JCRMI protokolo palaikymas, kuri leidžia J2ME taikomajai programai iškviesti metodą nutolusiame Java Card objekte.
- SATSA-PKI parašo paslaugų sąsaja – darbas su sertifikatais, duomenų pasirašymas, sertifikato pasirašymo užklausoje CSR¹⁷ generavimas.
- SATSA-CRYPTO kriptografinė sąsaja – apibrėžia šiame darbe jau minėtus Key ir PublicKey interfeisus bei KeyFactory, MessageDigest, ir Signature klases, taip pat

¹⁷ Certificate Signing Request

numato klases ir interfeisus duomenų kodavimui ir dekodavimui, parašo verifikavimui, žinutės santraukos skaičiavimui¹⁸.



16 paveikslas. SATSA programuotojo sąsajos [ORT05]

Išskiriami keli pagrindiniai SATSA trūkumai [KMH07]. Visų pirma, SATSA paprastai platinamas kaip Java vykdymo aplinkos JRE dalis. Kadangi JRE yra priklausoma nuo operacinės sistemos teikiamų paslaugų, vadinasi, telefono operacine sistema turi būti visiškai patikima. Kaip viena iš potencialių grėsmių yra įvardijamas PIN kodo, kuriuo paprastai būna apsaugotos SIM kortelėje realizuotos SATSA operacijos, įvedimas. Operacinėje sistemoje gali veikti šešėlinė programa, kuri fiksuoja kiekvieną klavišo paspaudimą; taip pat įvestas PIN kodas prieš perduodant jį š SIM kortelę saugumas atmintyje, kas taip pat sudaro galimybę jį nuskaityti piktavališkoms programoms. Kita galima grėsmė yra susijusi su komunikavimo kanalais. Kiekvienai J2ME taikomajai programai išskiriamas loginis kanalas bendravimui su intelektualiaja kortele. Toks kanalas gali būti pažeidžiamas per žemo lygio operacinės sistemos funkcijas. Pastarosios grėsmės leidžia daryti išvadą, kad taikomoji programa (J2ME midletas su SATSA) negali būti saugesnė nei operacinė sistema, kurioje ji veikia.

Kitas SATSA trūkumas – kliento sertifikatai negali būti naudojami autentifikacijai HTTPS komunikacijai naudojant SSL ar TLS protokolus. Taip pat pastebima, kad su SATSA atlikti parašo verifikavimą yra kur kas sudėtingiau nei pasirašyti duomenis. SATSA generuoja pasirašytus pranešimus naudojant kriptografinį žinutės sintaksės formatą CMS¹⁹.

¹⁸ Šioje sąsajoje SIM kortelė nedalyvauja, todėl veiksams su jautriais duomenimis atlikti rekomenduojama naudoti APDU/JCRMI sąsajas.

¹⁹ Cryptographic Message Syntax

Norint verifikuoti parašą, taikomoji programa visų pirma turi suskaidyti žinutę į parašo ir duomenų dalis bei pateikti viešąjį raktą. Egzistuoja trečiųjų šalių bibliotekos darbui su CMS formatu, tačiau būtų paprasčiau, jeigu SATSA gebėtų verifikuoti per tą pačią SATSA sąsają pasirašytas žinutes.

Dar vienas SATSA trūkumas, kurį apžvelgsime, yra skirtinga elgsena pasirašant duomenis ir verifikuojant jau pasirašytus duomenis. Pirmuoju atveju vartotojui grafinės sąsajos pagalba yra pateikiami pasirašomi duomenys, o antruoju – ne. Kitaip tariant, vartotojas abiem atvejais turėtų žinoti, kokie yra duomenys ir kartu pasitikėti SATSA. Kita problema yra sertifikato verifikavimo nepalaikymas. J2ME taikomųjų programų programuotojai patys turi realizuoti sertifikato verifikavimo procesą bei viešojo rakto išskyrimą iš sertifikato kartu pateikiant patį sertifikatą ir pasirašytus duomenis vartotojui. Kitais žodžiais sakant, SATSA pateikia bazinius elementus darbui su PKI, tačiau nepateikia sertifikato verifikavimo funkcionalumo, koks yra J2SE.

Verta paminėti ir tai, kad privatūs intelektualiojoje kortelėje saugomi raktai negali būti panaudoti duomenų atkodavimui, kadangi jie yra pasiekiami tik pasirašant duomenis.

Deja, SATSA / JSR177 šiuo metu palaiko tik labai nedidelę dalys mobiliųjų įrenginių. Dėl šios priežasties nėra nei vieno komercinio sprendimo, paremto SATSA technologija. Taip pat reikia turėti omenyje, kad atitinkamus SATSA numatytus ir per RMI sąsają pasiekiamus metodus turėtų realizuoti SIM kortelėje esantys objektai.

4.5. Išvados

Šiame skyriuje glaustai apžvelgėme pagrindinius technologijas, susijusias su mobiliuoju elektroniniu parašu bei lemiančias jo sudėtingumą. Atlikta Java Card saugumo sąsajų analizė leidžia daryti prielaidą, jog numatytų priemonių turėtų pilnai užtekti dokumento pasirašymui reikalingų funkcijų realizavimui Java Card SIM kortelėje. Toks sprendimas ne tik užtikrintų atitikimą saugumo standartams, bet ir užkirstų kelią uždarų sprendimų, specifinių konkretaus ryšio operatoriaus išduodamoms SIM kortelėms, diegimą.

Paprastumo dėlei nebuvo analizuoti esami komerciniai sprendimai, kurie vienokiu ar kitokiu būdu remiasi šiame skyriuje minėtais mechanizmais. Paprastai komercinių sprendimų dokumentacija būna konfidenciali, o viešai prieinamuose dokumentuose stokojama techninių detalių, kurios šiame darbe kaip tik ir yra svarbiausios.

Verta išskirti palyginti neseniai, 2002 m. ETSI instituto išleistą trijų standartų rinkinį MSS²⁰ apie mobilaus parašo paslaugą. Jame yra apibrėžiama mobiliojo parašo infrastruktūra,

²⁰ Mobile Security Service

aprašant kiekvieną jos komponentų, komunikavimą tarp jų SOAP protokolu, o taip pat mobilaus parašo pernešamumo²¹ koncepcija, kuri numato, kad mobilaus parašo transakcija, inicijuota konkrečios paslaugos tiekėjo, turi pasiekti mobiliojo parašo paslaugos tiekėją MMSP²² nepriklausomai nuo to, prie kurio mobiliojo ryšio tinklo vartotojas yra prisiregistravęs. Vienas populiariesnių komercinių mobilaus parašo sprendimų gamintojų *Valimo* teigia, kad jų produktai yra visiškai suderinti su ESS standartu.

Dar 2001 m. kaip pilotinis projektas startavęs kompanijos *SmartTrust* produktas *SmartSignature* kaip vieną iš tikslų kėlė tai, kad vartotojui m-komercijos transakciją aktyvuoti reikėtų ne daugiau vienos SMS žinutės [GC02]. Panašu, kad nors technologijos stipriai pažengė į priekį, šis principas yra vis dar labai aktualus, kadangi kaip jau minėta šiame darbe, nuo nešmenos nepriklausomas protokolas BIP yra palaikomas tik nedaugelio įrenginių, todėl SMS išlieka vieninteliu „patikimu“ transportu iki mobiliojo vartotojo²³.

Taip pat reiktų pastebėti, kad tam tikrų teisinių pasekmių gali sukelti faktas, jog vartotojui, kuris mobiliuoju telefonu pasirašo dokumentą, realiai nėra parodomas jo tekstas, o tik santrauka. Tai visų pirma sąlygoja jau minėtas SMS naudingojo tūrio apribojimas bei ribotų STK komandų galimybės atvaizduoti dokumentą telefono ekrane²⁴. Tačiau tai yra tik viena iš daugelio problemų, neminint tų, kurios iškyla integruojant kitus wPKI dalyvius - trečiąsias šalis (elektroninio parašo operatorius, sertifikavimo organizacijas, bankus, valstybines institucijas ir kt.) su mobiliojo ryšio operatoriaus infrastruktūra bei Vyriausybių keliamų reikalavimų teisinį įgyvendinimą.

²¹ Specifikacijoje naudojamas žodis *roaming*.

²² Mobile Signature Service Provider

²³ Su sąlyga, kad užklausa yra inicijuojama iš operatoriaus, t.y. *push* modelis.

²⁴ STK komandomis telefone galima atvaizduoti tik įprastą tekstą GSM koduote ar unikodu.

5. Tolimesni darbai

Atliktą išsamią pavyzdinės SIM kortelėje su Java Card platforma veikiančios StartDial taikomosios STK programos analizę bei aptartus pagrindinius mobiliojo elektroninio parašo technologinius aspektus galima panaudoti tolimesnei STK programų studijai.

Viena iš galimų tyrimo sričių būtų detalesnis OTA mechanizmų tyrimas, kurio rezultatas galėtų būti modelis, leidžiantis trečiosioms šalims (pavyzdžiui, pridėtinės vertės paslaugų tiekėjams – bankams, internetinėms parduotuvėms ir pan.) saugiai bendrauti su SIM kortele, užtikrinant tiek atitikimą standartams, tiek saugumą visuose bendravimo lygiuose (operatoriaus sistemose, mobiliajame telefone ir pačioje SIM kortelėje). Akivaizdu, kad esamas OTA komunikavimas per SMS nėra efektyvus, kadangi didesnių duomenų perdavimas užtrunka ilgai, be to, žinučių fragmentavimas yra jautrus ryšio praradimui, t.y. jeigu siunčiant pranešimo fragmentus SMS žinutėmis gavėjas tampa nepasiekiamas, gali tekti pakartoti ne konkretų fragmentą, tačiau visą pranešimą. Šiame darbe minėtas BIP protokolas arba jo alternatyva – šiame darbe jau nagrinėta *LAUNCH BROWSER* proaktyvi komanda ir platesnis jos panaudojimas galėtų eliminuoti šias problemas.

Vertingas tolimesnių tyrimų objektas taip pat galėtų būti išsami naujų standartų (JSR177, UICC – 3G SIM kortelės, fizinės prieigos prie SIM kortelės) analizė. Dabar galima tikėtai prognozuoti, kurios iš naujovių įsigalės, t.y. užims pakankamą rinkos dalį, kad tomis technologijomis būtų galima realizuoti konkrečius sprendimus. Vienas iš pavyzdžių – Apache Triplesec projektas, kuris mobiliąjį telefoną paverčia vienkartinio slaptažodžio (OTP – One Time Password) generatoriumi. Šį sprendimą integravus su SIM kortele SATSA pagalba leistų turėti visiškai patikimą slaptažodžių generatorių, kuris galėtų pakeisti esamus, išduodamus bankų ar kitų institucijų.

Paskutinė galima tyrimų sritis – tai telefono taikomosioms programoms (MMS žinutėms, WAP naršyklei, vaizdo bei garso transliacijų grotuvui, kontaktų sinchronizacijai ir t.t.) skirti nustatymai. Tai reiškia, kad mobiliojo ryšio vartotojas, SIM kortelę įdėjęs į kitą telefono įrenginį, turėtų korektiškus tinklo nustatymus. Šioje situacijoje Java Card apletas galėtų pasitarnauti taikydamas telefono savybių atpažinimo mechanizmus pasinaudojant telefono profilio informacija ir, priklausomai nuo telefono savybių, nustatymų failą užpildyti reikalinga informacija.

Išvados

Šiame magistro darbe buvo išanalizuoti literatūros šaltiniai, susiję su SIM kortele, jos sandara, standartais, STK, svarbiausiais Java Card aspektais bei SIM kortelės duomenų valdymu nuotoliniu būdu, naudojant OTA mechanizmus. Pagrindinė šio darbo dalis buvo skirta pavyzdinės STK taikomosios programos, veikiančios Java Card SIM kortelėje, projektavimui ir programavimui. Tai yra StartDial projekto, kuris taip pat buvo pristatytas tarptautiniame SIMAGINE 2006 konkurse pasaulinio GSM kongreso Barselonoje metu ir užėmė antrąją vietą [SIM06], sudedamoji dalis. Darbe taip pat buvo išnagrinėtos svarbiausios su mobiliuoju elektroniniu parašu susijusios technologijos, įvardijant kiekvienos iš jų privalumus ir trūkumus bei pateikiant pasiūlymus kai kurių specifinių problemų sprendimui.

Įvardinsime tris pagrindinius šio darbo rezultatus: atlikta ir pateikta išsami susisteminta abonento atpažinimo modulio įrankių rinkinio technologijų studija, realizuotas sudėtingas Java Card technologija paremtas STK projektas, pristatant jo technologinius ir projektinius sprendimus, kartu pademonstruojant realų jo veikimą bei išsigilinta į mobilaus elektroninio parašo technologijas. Pasiekus minėtus rezultatus, kurie ir buvo pagrindinis šio darbo tikslas, galima daryti tam tikrus apibendrinimus ir pasiūlymus.

Visų pirma pastebėsime, kad SAT SIM technologijų sudėtingumą visų pirma lemia jos uždarumas. Pagrindinis informacijos šaltinis, susijęs su SIM, STK, Java Card ir OTA technologijomis vis dėlto yra tarptautiniai standartai, dažnai aprašantys tik bendrus panaudojimo principus, todėl atliekant StartDial projektą su daugeliu jų teko ne tik detaliam susipažinti, bet ir palyginti, suderinti, o pačios programos realizacija pareikalavo išsigilinti į visą eilę techninių detalių, kurios paaiškėjo tik atliekant projektą. Jau minėjome, kad nėra paprasta rasti dokumentuotą pavyzdinę STK programą, todėl tiek atvirai pateikiami sprendimai, tiek programinė įranga bei literatūra atvertų kelią platesniam STK galimybių panaudojimui. Kaip pavyzdį būtų galima pateikti J2ME technologiją, kurią palaiko dauguma šiandieninių mobiliųjų telefonų ir kuriai kurti yra laisvai prieinama visa eilė integruotų įrankių, o problemų sprendimą neretai palengvina atviri forumai, kuriuose dalyvauja programuotojai iš viso pasaulio.

Šiame darbe pristatytas StartDial projektas sprendžia vieną specifinę problemą – mobilaus telefono vartotojo skambučius tam tikrais numeriais pakeičia telefono WAP naršyklės paleidimu su adresu, susietu su skambinamuoju numeriu, taip palengvinant mobiliojo interneto pasiekimą. Nepaisant to, principinius projekto metu gautus sprendimus galima pritaikyti ir kitoms probleminėms sritims, taip pat ir mobiliam elektroniniam parašui. Darbe pabrėžėme, kad Java Card technologijos naudojimas wPKI infrastruktūros

elemente – SIM kortelėje – užtikrintų platesnį suderinamumą bei atitikimą standartams. Kaip žinia, šiuo metu skirtingi Lietuvos mobiliojo ryšio operatoriai naudoja skirtingų gamintojų SIM korteles. Tai reiškia, kad STK paremta elektroninio parašo pasirašymo taikomoji programa ir galimi jos atnaujinimai turėtų būti suderinti su kiekviena iš naudojamų SIM kortelių, o tai gali būti labai sudėtingas uždavinys. Visgi reikia pastebėti, kad dauguma šiuo metu gaminamų SIM ar USIM kortelių yra būtent su Java Card platforma, todėl iš esmės tai neturėtų pareikalauti papildomų investicijų. Tuo tarpu vienas pagrindinių Java Card panaudojimo elektroninio parašo STK programai privalumų būtų tai, kad atsiradus naujiems poreikiams būtų užtikrinta, jog ne vienas kuris nors wPKI dalyvaujantis operatorius „laimi“ pateikdamas papildomą funkcionalumą, bet kad bet kokie pakeitimai vienodu principu yra diegiami visų wPKI dalyvaujančių ryšio tiekėjų klientų SIM kortelėse.

Paskutinis minėtinas dalykas yra pati SIM kortelės technologija, kuri, palyginti su kitomis mobiliosiomis technologijomis, beveik neprogresuoja ir yra sąlyginai pasenusi. Tas pats SIM modulis vis dar yra naudojamas tiek dešimties metų senumo mobiliajame telefone, tiek delniniame telefone-kompiuteryje, palaikančiame vaizdo telefoniją, bevielę WiFi technologiją ir kt. Nors jau egzistuoja realiai veikiančios SIM kortelės su 1 GB dydžio EEPROM atmintimi ir jose įdiegtu žiniatinklio serveriu, taip pat baigiama standartizuoti keliasdešimt kartų greitesnė USB²⁵ sąsaja tarp telefono ir SIM kortelės, pakeisianti dabartinę ISO 7816, praeis nemažai laiko, kol šias naujoves palaikys mobilieji įrenginiai. Šalia to svarbu pastebėti, kad SIM modulis buvo ir liks saugia laikmena, kurios savininkas, priešingai nei mobilaus įrenginio, yra tą SIM kortelę išdavęs ryšio operatorius. Šiuo požiūriu perspektyvias SIM paremtas paslaugas galėtume laikyti tas, kurioms reikalingos saugios operacijos, susietos su SIM kortelės turėtojo tapatumu ir naudojamos autorizacijai, autentiškumo patvirtinimui bei saugių transakcijų patvirtinimui. Šiame darbe išnagrinėjome vieną iš pavyzdžių – elektroninį parašą mobiliojoje aplinkoje, tačiau lygiai taip pat galima galvoti apie prieigą prie bevielio WiFi ryšio taškų SIM kortelės pagalba, biometrines paslaugas ir nemažai kitų.

Tikimasi, kad šio magistro darbo metu surinkta medžiaga galėtų pasitarnauti kaip tam tikras įvadas tiems, kurie dirba su darbe nagrinėjamomis technologijomis.

Atliekant šį darbą buvo vadovautasi moksliniais straipsniais, tarptautiniais standartais ir kita nurodyta literatūra, konsultacijomis su mobiliojo ryšio operatoriais, SIM kortelių gamintojais bei tik SIMAGINE konkurso dalyviams prieinamuose forumuose pateikiama

²⁵ Šiuo metu vis dar svarstoma dėl USB, MMC arba abiejų sąsajų palaikymo standartizavimo.

informacija. Darbo metu buvo pasinaudota SIMAGINE konkurso organizatoriaus suteiktomis priemonėmis: integruotu darbui su SIM kortelėmis skirtu įrankių rinkiniu [VIEWS] bei Java Card SIM kortelėmis.

Summary

This master thesis presents the detailed analysis of the SIM Smart Card, the SIM Application Toolkit and related technologies. Initially provided with an overview of important sources, standards and other materials related to STK technologies this thesis focuses on sample Java Card based STK project StartDial which translates a dialed number into an URL.

The StartDial solution innovatively utilizes the simple “dialing” interface to launch pre-defined mobile internet sites / VAS services, in essence creating a “speed dial” for the mobile internet and providing instant gratification to the users. By using the StartDial technology, accessibility and usability of mobile sites is radically improved, leading to increased number of satisfied users and more revenue both for operators and for the site owners. StartDial architecture is based on SIM resident Java Card applet which intercepts MO calls or SS strings by listening to “CALL CONTROL BY SIM” events and launches the phone’s WAP browser with the URL depending on the dialed short code. The URLs are stored on the SIM card linear-fixed records file and are updated regularly via OTA. Backend system contains database storing URLs and is responsible for synchronization with SIM cards via OTA. Over-the-Air transactions are used to convey shortcuts information to subscribers. An in-house TLV based protocol has been developed to convey shortcut information. The protocol message consists of operation tags which might be one of *update*, *insert* or *delete*, length information and the shortcut, shortcut name and value (URL). A working prototype was successfully tested with a few handset models manufactured by each of the leading handset manufacturers: Nokia, Sony-Ericsson, Siemens and Motorola. Both core and additional (such as auto completion) StartDial functions were found to work as expected on the newer mobile handsets supporting letter class “c”, which includes the LAUNCH BROWSER proactive command.

Last part of this thesis is dedicated to the mobile digital signature and related technologies. It deals both with STK and Java Card applications security including new JSR 177 / SATSA specification – an enabler for J2ME application to access the Smart Card.

Literatūros ir šaltinių sąrašas

- [DGSW02] Dankers, J.; Garefalakis, T.; Schaffelhofer, R.; Wright, T. Public key infrastructure in mobile systems. *Electronics & Communication Engineering Journal*, Vol.14, Iss.5, Oct 2002. Pages: 180-190.
- [NL04] S. Nambiar, C.T. Lu. Analysis of payment transaction security in mobile commerce. *Information Reuse and Integration*, 2004. IRI 2004. Proceedings of the 2004 IEEE International Conference on Volume, Issue , 8-10 Nov. 2004. Pages: 475-480.
- [BU04] Mohamad Badra, Pascal Urien. Toward SSL Integration in SIM SmartCards. *IEEE Wireless Communications and Networking Conference 2004*. Atlanta (Georgia, USA), March 2004.
- [HK]CS02] J.H. Han, Y.J. Kim, S.I. Jun, K.I. Chung, C.H. Seo. Implementation of ECC/ECDSA cryptography algorithms based on Java card. *Distributed Computing Systems Workshops*, 2002. Proceedings. 22nd International Conference on, Vol., Iss., 2002. Pages: 272-276.
- [KMH07] A.N. Klingsheim, V. Moen, K.J. Hole. Challenges in Securing Networked J2ME Applications. *Computer*, Vol.40, Iss.2, Feb. 2007. Pages: 24-30.
- [JJ06] S. Jain, A. Jain. SIM Application Toolkit - Protocol Conformance and Implementation Challenges. *Wireless and Mobile Communications*, 2006. ICWMC '06. International Conference on, Vol., Iss., July 2006. Pages:47-47.
- [UND03]. V. Undzėnas. ELEKTRONINĖ KOMERCIJA (Elektroninio parašo klausimai). Mokymo priemonė. VU MIF Programų sistemų katedra. Vilnius, 2003.
- [GC02] Scott B. Guthery, Mary J. Cronin. *Mobile Application Development with SMS and the SIM Toolkit*. McGraw-Hill, 2002.
- [RE04] Wolfgang Rankl and Wolfgang Effing. *Smart Card RE04*, 3rd edition. John Wiley & Sons, 2003.
- [ISO 7816-4] ISO/IEC 7816-4:1997 Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry command for interchange.
- [GSM 02.19] Digital cellular telecommunications system (Phase 2+, Release 98): Subscriber Identity Module Application Programming Interface (SIM API); Service description; Stage 2. ETSI, Sophia Antipolis, France, 1999.
- [GSM 03.19] Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™ ; Stage 2. ETSI, Sophia Antipolis, France, 1999.
- [GSM 03.48] Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2. ETSI, Sophia Antipolis, France, 1999.

- [GSM 11.11] European digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.11). ETSI, Sophia Antipolis, France, 1998.
- [GSM 11.14] European Digital cellular telecommunications system (Phase 2+): Specification of the SIM application toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface (GSM 11.14). ETSI, Sophia Antipolis, France, 1998.
- [WIM] Wireless Application Protocol Forum. Wireless Identity Module. Part: Security. WAP-260-WIM-20010712-a. Version 12-July-2001.
- [JCSPEC] Java Card Platform Specifications. Sun Microsystems. URL: <http://java.sun.com/products/javacard/specs.html>.
- [JC222] Java Card™ Specifications, Version 2.2.2. Release Notes. March 2006. URL: http://java.sun.com/products/javacard/RELEASENOTES_jcspecspw_2_2_2.html.
- [ISS06] SIM Alliance. Interoperability Stepping Stones Release 6. URL: <http://www.simalliance.org/>.
- [VIEWS] SIM cards and applications - software tools. VIEWS Developer. Axalto. URL: http://www.axalto.com/wireless/views_developer.asp.
- [WIT01] Marc Witteman. Smartcard Security. Information Security Bulletin, October 2003. CHI Publishing Ltd.
- [SMTRUST] Commercially proven OTA platform. SmartTrust. URL: <http://www.smarttrust.com/>.
- [E3P] Elektroninio Parašo Proveržio Programa (E3P). URL: <http://www.signature.lt>.
- [JSR177] JSR 177: Security and Trust Services API for J2ME. URL: <http://jcp.org/en/jsr/detail?id=177>.
- [ORT05] C. Enrique Ortiz. The Security and Trust Services API for J2ME, Part 1. March 2005. URL: <http://developers.sun.com/techttopics/mobility/apis/articles/satsa1/>.
- [NAC06] Armand Nacheff. J2ME – JSR 177. SIMagine University. 22/08/2005 A.N. URL: http://www.simagine.axalto.com/summer2006pdf/SIMagine_JS177-presentation2.pdf.
- [SIM06] Simagine 2006 Results. URL : http://www.simagine.axalto.com/simagine2006_results.asp
- [RTN01] Ryšių technikos naujienos. Vilnius. 2001 m.

Priedas nr. 1. StartDial testinių duomenų paruošimo skriptas

```
#!/usr/bin/env python

import sys
from struct import pack

# Žymių kodai

ST_TAG_NAME      = 0xF0;
ST_TAG_SHORTCUT  = 0xF1;
ST_TAG_URL       = 0xF2;

ST_CMD_NEW       = 0xF3;
ST_CMD_UPD       = 0xF4;
ST_CMD_DEL       = 0xF5;

# Pradiniai duomenys

data = [
    {
        ST_TAG_SHORTCUT:    "122",
        ST_TAG_NAME:        "Google Search",
        ST_TAG_URL:         "http://wap.google.com"
    },
    {
        ST_TAG_SHORTCUT:    "123",
        ST_TAG_NAME:        "Online Weather",
        ST_TAG_URL:         "http://wap.onlineweather.com"
    },
]

# Paketo formavimas

packet = ""

for val in data:
    tmp = ""
    for cmd in [ST_TAG_SHORTCUT, ST_TAG_NAME, ST_TAG_URL]:
        t = cmd
        v = val[cmd]
        l = len(v)
        tmp += pack("2B", t, l)

        if t == ST_TAG_SHORTCUT:
            for c in v: tmp += pack("B", int(c))
        else:
            tmp += pack("%ds" % l, v)

    packet += pack("2B%ds" % len(tmp), ST_CMD_NEW, len(tmp), tmp)

for c in packet:
    sys.stdout.write("%02X" % ord(c))
print
```